Windows NT Server 4.0 Upgrade Guide

Moving from Windows NT 4.0 Server to Windows Server 2003

Microsoft Corporation

Published: June 2003

Abstract

This guide is designed to help customers make the transition from a Microsoft Windows NT® Server 4.0 environment to the Microsoft Windows Server™ 2003 operating system. The information presented here is intended for both developers and administrators, but the emphasis is on providing support information for system administrators. This guide explains critical considerations when upgrading and the steps required to migrate to Window Server 2003.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Part 1: Planning Your Migration **1**

Introduction **2**

Upgrade Roadmap 2

Why Upgrade? 3

Top 10 Reasons to Upgrade 4

Preparing to Upgrade **8**

Determining the Supported Software Upgrades 8

Upgrading with Exchange 2000 9

Upgrading with Microsoft SQL Server™ 7.0 9

Hardware Considerations 9

Windows Server 2003 Minimum System Requirements 12

Assessing and Documenting Server Upgrade Order 13

Server Upgrade Checklists 15

Assessing Application Compatibility **19**

About ACT 3.0 19

Installing ACT 3.0 19

Making an Inventory with Collector 20

Sample Application Inventory with Collector 21

Using Analyzer 1.0 23

What's Next? 29

Upgrading Windows NT 4.0 Servers **30**

Upgrading Windows NT 4.0 Stand-alone Servers 30

Upgrading Windows NT 4.0 Member Servers 30

Sample In-Place Upgrade for a Windows NT PDC 35

Results of the Sample Windows NT Upgrade 41

Sample Product Activation 43

Migrating to Active Directory **45**

Benefits of Active Directory 45

Improved Management with Group Policy 46

Windows NT Server 4.0 Upgrade Design and Planning 47

Connectivity with Windows NT Server 4.0, Windows 2000, and Windows Server 2003 49
Upgrading a Windows NT Domain to Active Directory 53
Sample Active Directory Migration Plan 63
Results of the Upgrade 75
Sample Upgrade Review 77
Part 2: Understanding Key Windows Server 2003 Components 80
Windows Services 81
New Services in Windows Server 2003 81
Setting Server Roles with the Configure Your Server Wizard 81
Starting and Stopping Services with the MMC 82
Service Security Contexts 84
Svchost for Starting Services 87
Security Changes Under Windows Server 2003 91
Goals of the Trustworthy Computing Initiative 91
IIS 6.0 Security Changes 92
New Security-Related Policy Changes 95
COM+ Security and Active Directory 97
Security Enhancements in the .NET Framework 98
Security-Related Enhancements for Authentication 99
Security Enhancements for Access Control 102
Network Security 103
TCP/IP and Support for Earlier Networking Protocols 105
NetBEUI 105
Data Link Control (DLC) 105
Quality of Service and RSVP Signaling 106
Dial-in Support: IPX and AppleTalk 106
Streams 106
Part 3: Application Compatibility Considerations 107
Internet Information Services (IIS) 6.0 108
IIS 6.0 Reliability and Availability 108
IIS 6.0 Manageability 109
IIS 6.0 Security 109

Major Differences Among Versions of IIS 110
Isolation Modes 111
Applications After Upgrade 118
ISAPI Extension Settings 119
ISAPI Filters Removed 120
Upgrading ASP Web Applications 120
Upgrading ASP Web Applications to ASP.NET Applications 121
ASP.NET 1.0 Applications and ASP.NET 1.1 Applications 121
Exchange Server 122
Exchange 2000 and Exchange 2003 Considerations 122
Upgrading to Exchange Server 2000 127
Features Made Obsolete by Upgrading 128
Upgrade Paths for Exchange Server 2003 128
COM+ 1.5 130
Feature Changes from Previous Releases 130
New Features in COM+ 130
Side-by-side Deployments of .NET Framework 1.0 and 1.1 132
How Side-by-Side Versions Work 132
Assemblies and Side-by-Side Execution 132
Changes that Affect Backward or Forward Compatibility 133
Benefits of Side-by-Side Execution 134
Appendix A: Sample Active Directory Upgrade 136
Appendix B: Sample Log File from Compatibility Check 147
Appendix C: Related Links 150

Part 1: Planning Your Migration

Introduction

There are many ways to approach the task of performing an upgrade from Microsoft® Windows NT® Server 4.0 operating system environments to a Microsoft Windows Server™ 2003 environment. Each upgrade has to be analyzed and planned to determine the best possible approach for a specified scenario. This guide provides several scenarios to help you plan and execute an upgrade process in your organization.

When deciding how to upgrade, many questions must be addressed. What are the supported upgrade paths from Windows NT Server 4.0 to the desired version of Windows Server 2003, whether that is Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; or Windows Server 2003, Web Edition? Will existing applications running on Windows NT Server 4.0 run on Windows Server 2003? What factors determine the order of Windows NT server upgrades? Is there a need to upgrade the domain to the Microsoft Active Directory® directory service? Is Microsoft Exchange Server a consideration for your upgrade?

This guide was written to address these questions. The guide is structured as follows:

- **Part 1** provides a roadmap for upgrading Windows NT Server 4.0 to Windows Server 2003. The roadmap starts with planning and implementation and includes four main topics: preparing to upgrade, assessing application compatibility, starting an upgrade process for Windows NT 4.0 servers, and understanding requirements for upgrading to Active Directory.
- **Part 2** discusses key operating system changes, including changes to Windows services and security issues.
- **Part 3** addresses specific application compatibility considerations for Internet Information Services (IIS), Exchange Server, COM+, and the Microsoft® .NET Framework.

This guide is designed to help customers make the transition from Windows NT Server 4.0 to Windows Server 2003. The guide addresses both developer and administrator topics, but the emphasis is on providing support information for system administrators. Sample scenarios are provided with detailed walk-throughs that demonstrate the necessary considerations and practical approaches to upgrading to Window Server 2003.

Upgrade Roadmap

This guide provides a roadmap of the different ways an upgrade can be accomplished. Generally speaking, an upgrade to Windows Server 2003 can be approached in two ways:

- You can perform an in-place upgrade of Windows NT Server 4.0 to Windows Server 2003.
- You can perform a clean installation of Windows Server 2003, and then install the required applications.

In many cases, a clean installation is preferred to perform common tasks such as repartitioning drives, removing any unnecessary or unused files, and disabling any unnecessary services. Although an upgrade can be performed in such a way that existing application configuration settings are preserved, the preferred approach is a clean installation.

Planning is the first step in any major undertaking. The following steps are the recommended order in which to accomplish a successful migration from Windows NT Server 4.0 to Windows Server 2003:

- **Plan and implement.**
  - Prepare to upgrade.
  - Assess application compatibility with the Application Compatibility Toolkit 3.0.
  - Upgrade Windows NT 4.0 servers.
  - Implement Active Directory.
- **Assess fundamental operating system changes.**
  - Understand changes to Windows services.
  - Know which protocols are no longer supported.
  - Understand the ramifications of security changes.
- **Provide application support.**
  - Work with IIS 6.0.
  - Consider which version of Exchange Server to use.
  - Understand changes in COM+ 1.5.
  - Upgrade from .NET Framework 1.0 to .NET Framework 1.1.

Why Upgrade?

There are many reasons to upgrade. One reason is to keep pace with new technology. However, the time and financial investment in making a change can be substantial, even when upgrading a single computer. The return on investment must be evaluated. Windows Server 2003 provides many advantages over earlier Windows server versions. Many of these benefits fall under the umbrella of enhancing system security. Other significant new features help make this version of Windows the most reliable, scaleable, and dependable operating system that Microsoft has delivered. As a result, the return on investment of moving to Windows Server 2003 can be quickly realized.

New features include a completely rearchitected version of IIS 6.0 with ASP.NET and improvements to Active Directory that ease management, including cross-forest trusts and Active Directory in Application Mode (AD/AM). Other features include Volume Shadow Copy service for making point-in-time copies of critical data that can be used for restoration or archival purposes, integrated public key infrastructure (PKI) support using Kerberos 5.0, improved Terminal Services, clustering with 8-node support, and intelligent file services.

The following table summarizes the key benefits of upgrading.

Key Benefits

Benefit	Description
Reduce costs	Case studies have shown that organizations can recoup the cost of upgrading to Windows Server 2003 in 6 to 18 months with a 20 to 30 percent reduction in total cost of ownership. Windows Server 2003 has a 50-percent improved uptime over Windows NT Server 4.0 and reduces costs by reducing down time. New features such as the Volume Shadow Copy service have shown to reduce file recovery incidents by 90 percent.
Reduce risk	Security enhancements to Windows Server 2003 help reduce risk by keeping the system more secure than in previous versions and by ensuring mission-critical data is better protected than it was in previous versions. § To reduce the surface area exposed to an attacker, many services are no longer installed by default and many run with reduced permissions. § Software Restriction Policies help to mitigate security risks by preventing users from executing harmful applications. § Studies have shown that approximately 60 percent of corporate data is stored on the desktop, unprotected. New features in Windows Server 2003 help to protect the computers that are on your network by redirecting where the My Documents data is stored: on the server as encrypted files. This change also facilitates more efficient backup through Shadow Copy services.
Increase productivity	Many features of Windows Server 2003 have significant performance improvements over Windows NT Server 4.0. Improvements have been measured for file, Web, directory, and transaction services compared to Windows NT Server 4.0.
Take advantage of the migration ecosystem	Powerful tools are available to help ensure a successful upgrade, including: § IIS 6.0 migration tool § Active Directory Migration Tool (ADMT) § Application Compatibility Toolkit 3.0 § Remote Installation tool § Automated Deployment Services § Many other tools available by third-party vendors

Top 10 Reasons to Upgrade

Here are the major new features and improvements for organizations considering upgrading from Windows NT Server 4.0:

1. Active Directory

Active Directory simplifies the administration of complex network directories and makes it easy for users to locate resources on even the largest networks. This enterprise-class directory service is scalable, built from the ground up using Internet-standard technologies, and fully integrated at the operating-system level in Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; and Windows Server 2003, Datacenter Edition.

Windows Server 2003 provides numerous ease-of-use improvements to Active Directory and new features, including cross-forest trusts, the ability to rename domains, and the ability to deactivate attributes and classes in the schema so that their definitions can be changed.

2. Group Policy

Administrators can use Group Policy to define the settings and allowed actions for users and computers. In contrast with local policy, Group Policy can be used to set policies that apply across a specified site, domain, or organizational unit in Active Directory. Policy-based management simplifies such tasks as system update operation, application installation, user profiles, and desktop-system lockdown.

The Group Policy Management Console (GPMC) provides a new framework for managing Group Policy. With GPMC, Group Policy becomes much easier to use, a benefit that enables more organizations to better use Active Directory and take advantage of its management features.

3. Server Performance

In internal tests, Windows Server 2003 shows dramatic performance gains over previous versions of Windows server operating systems. For example, file and Web server performance is two times faster than Windows NT Server 4.0. While an organization's performance gains may vary because of unique network and computer settings, Microsoft is confident that the improved performance of Windows Server 2003 will help deliver faster service for network solutions.

4. Shadow Copies of Shared Folders

As part of Volume Shadow Copy service, this feature enables administrators to configure point-in-time copies of critical data volumes without service interruption. These copies can then be used for service restoration, archival purposes, or restoration. Users can retrieve archived versions of their documents that are transparently maintained on the server. Productivity is improved by the ability to better recover documents.

5. IIS 6.0 and the .NET Framework

IIS 6.0 is a full-featured Web server that enables Web applications and XML Web services. IIS 6.0 has been completely rearchitected with a new fault-tolerant process model that greatly boosts the reliability of Web sites and applications.

Now, IIS can isolate an individual Web application or multiple sites into a self-contained process (called an application pool) that communicates directly with the operating system kernel. This feature increases throughput and capacity of applications while offering more headroom on servers, effectively reducing hardware needs. These self-contained application pools prevent one application or site from disrupting the XML Web services or other Web applications on the server.

IIS also provides health monitoring capabilities that discover, recover, and help prevent Web application failures. On Windows Server 2003, ASP.NET natively uses the new IIS process model. These advanced application health and detection features are also available to existing applications running under IIS 4.0 and IIS 5.0, and most applications do not need tp be modified.

The .NET Framework provides the programming model for building, deploying, and running Web-based applications and XML Web services in the IIS environment. It provides a productive, standards-based, multiple-language environment for integrating existing

investments with next-generation applications and services as well as the agility to solve the challenges of deployment and operation of Internet-scale applications. Existing applications can be repackaged as XML Web services, and UNIX applications can be integrated or even upgraded into the solution with less work than in the past.

6. Terminal Services

Terminal Server enables administrators deliver Windows-based applications, or the Windows desktop itself, to virtually any computing device—including those that cannot run Windows. When users run an application on Terminal Server, the application execution takes place on the server, and only keyboard, mouse, and display information is transmitted over the network. Users see only their own individual sessions, which are managed transparently by the server operating system, and remain independent of any other client session.

Remote Desktop for Administration builds on the remote administration mode of Windows 2000 Terminal Services. In addition to the two virtual sessions that are available in Windows 2000 Terminal Services remote administration mode, an administrator can also remotely connect to the real console of a server.

Terminal Server can enhance an enterprise's software deployment capabilities for a variety of scenarios that remain difficult to solve using traditional application distribution technologies.

7. Clustering (8-Node Support)

Available only in Windows Server 2003, Enterprise Edition and Windows Server 2003, Datacenter Edition, this service provides high availability and scalability for applications such as databases, messaging systems, and file and print services. Clustering works by enabling multiple servers (nodes) to remain in constant communication. If one of the nodes in a cluster becomes unavailable as a result of failure or maintenance, another node immediately begins providing service, a process known as failover. Users who are accessing the service continue their activities, unaware that service is now being provided from a different server (node).

Both Windows Server 2003, Enterprise Edition and Windows Server 2003, Datacenter Edition, support server cluster configurations of up to eight nodes.

8. Integrated PKI Support Using Kerberos 5.0

Using Certificate Services and certificate management tools, organizations can deploy their own PKI. With PKI, administrators can implement standards-based technologies, such as smart card logon capabilities, client authentication using Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, e-mail security improvements, digital signatures, and connectivity through Internet Protocol security (IPSec).

Using Certificate Services, administrators can set up and manage certification authorities that issue and revoke X.509 V3 certificates. This means that organizations do not have to depend on commercial client authentication services, although they can be integrated into an organization's PKI.

Kerberos 5.0 is a mature, industry-standard network authentication protocol. With Kerberos 5.0 support, a fast, single-logon process gives users the access they need to enterprise resources, as well as to other environments that support this protocol. Additional benefits

include mutual authentication, where a client and server must both provide authentication, and delegated authentication, where a user's credentials are tracked end-to-end.

9. Command-Line Management

The Windows Server 2003 family provides a significantly enhanced command-line infrastructure, which enables administrators to perform most management tasks without using a graphical user interface. Of special importance is the ability to perform a wide range of tasks by accessing the information store enabled by Windows Management Instrumentation (WMI). This WMI command-line (WMIC) feature provides a simple command-line interface that interoperates with existing shells and utility commands and can be easily extended by scripts or other administration-oriented applications.

Overall, the greater command-line functionality in the Windows Server 2003 family, combined with ready-to-use scripts, rivals the power of other operating systems often associated with higher cost of ownership. Administrators accustomed to using the command line to manage UNIX or Linux systems can continue managing from the command line in the Windows Server 2003 family.

10. Intelligent File Services

Encrypting File System (EFS) enables users to encrypt and decrypt files to help protect them from intruders who might gain unauthorized physical access to their sensitive, stored data (for example, by stealing a laptop or external disk drive). Encryption is transparent—users work with encrypted files and folders just as they do with any other files and folders. If the EFS user is the same person who encrypted the file or folder, the system automatically decrypts the file or folder when the user accesses it later.

Distributed File System (DFS) simplifies the task of managing shared-disk resources across a network. Administrators can assign logical names to the shared drives on a network, rather than requiring users to know the physical name assigned to each server they need to access.

File Replication Service (FRS) is a significant improvement over the directory replication feature in Windows NT Server 4.0. For example, FRS provides multiple-master file replication for designated directory trees between designated servers. FRS is also used by DFS to synchronize content between assigned replicas, and by Active Directory to synchronize content from the system volume information across domain controllers.

Preparing to Upgrade

Before beginning an upgrade from Windows NT Server 4.0 to Windows Server 2003, you need a plan that details the many tasks to be performed. If the upgrade includes Active Directory, even more planning is recommended. Your upgrade plan assists in establishing the order in which to upgrade servers and domains, assessing available resources, and obtaining the information necessary to upgrade the systems in the most efficient way.

Your upgrade plan should also include all components to be upgraded and the proper upgrade order. Dependencies among servers and applications need to be carefully examined. Hardware needs to be inspected as well. Can the current servers be upgraded or does new hardware need to be purchased? Are there any applications that need to be upgraded? Are there any servers that cannot be upgraded?

Organizations can benefit from upgrading individual servers to Windows Server 2003 as well as upgrading all servers. In this section of the guide, you'll find information to help plan the hardware and server migration order.

Determining the Supported Software Upgrades

To start, you must identify the operating systems that are running in the environment and determine whether those computers can be upgraded to Windows Server 2003 or whether a clean operating system installation must be performed.

To upgrade a Windows NT Server 4.0 computer to Windows Server 2003, Service Pack 5 (SP5) or later must be installed. In fact, unless there is a known issue with a service pack, it is best to install the latest service pack for the Windows NT Server 4.0 as well as any other applications that may run on the Windows NT 4.0 servers.

The following table lists the Windows NT Server 4.0 operating systems and whether they can be upgraded directly to different versions of Windows Server 2003. When performing an upgrade to Windows Server 2003, most applications do not need to be reinstalled.

Upgrade Paths for Windows NT Server Versions

Current Operating System Version	Upgrade Version		
	Windows Server 2003, Standard Edition	**Windows Server 2003, Enterprise Edition**	**Windows Server 2003, Datacenter Edition**
Windows NT 4.0 Server, Standard Edition	X	X	
Windows NT 4.0 Server, Enterprise Edition		X	

If there are computers running operating systems that cannot be upgraded directly to a version of Windows Server 2003, do one of the following:

- Upgrade the computer to run an operating system that can be upgraded to Windows Server 2003.
- Perform a clean installation of Windows Server 2003 on those computers.

Upgrading with Exchange 2000

Because of significant changes in Windows Server 2003 security and other features, Exchange Server 2003 is the only Exchange version capable of running on this operating system. However, at the time this guide was written, Exchange Server 2003 was not yet available. (It will be released later in 2003.) Moreover, Exchange 2000 cannot be installed or run on a server that is running Windows Server 2003. Exchange 2000 must be installed on a server that is running Windows 2000 Server. Fortunately, this platform—Exchange 2000 and Windows 2000—can coexist in a Windows Server 2003 environment.

If you are considering whether to upgrade your Windows–based servers to Windows Server 2003, rest assured that doing so will not disrupt an existing messaging infrastructure. File and print servers, domain controllers, and global catalog servers can be upgraded to Windows Server 2003 with no adverse impact on Exchange operations.

Upgrading with Microsoft SQL Server™ 7.0

In an effort to provide customers with security-enhanced products, Microsoft supports only SQL Server 2000 with Service Pack 3 (SP3) or later and MSDE 2000 with SP3 or later on Windows Server 2003. SQL Server 7.0 and MSDE 1.0 are not supported on Windows Server 2003. It is recommended that customers who run applications with SQL Server 7.0 and MSDE 1.0 should evaluate and upgrade to SQL Server 2000 and SQL Server Desktop Engine (also known as MSDE 2000) respectively with SP3 on Windows Server 2003.

For more information on SQL Server support and upgrade information, see “Running SQL Server on Windows Server 2003” on the SQL Server Web site at http://www.microsoft.com/sql/howtobuy/windowsnetsupport.asp.

Hardware Considerations

As part of your upgrade plan, review and document the existing hardware configuration and operating system of each domain controller that you want to upgrade. Use this information to identify the computers that you can upgrade to Windows Server 2003 and the computers that you must decommission or return to member server status. Keep decommissioned servers for rollback servers in the event that you must roll back the upgrade.

Hardware and Driver Compatibility

It is a good idea to determine whether a system’s hardware is on the Hardware Compatibility List. If not, search the hardware manufacturer’s Web site for updated drivers. When a driver is found, check it for a signature. Driver signing is a multifaceted process in which device drivers are verified through a series of tests administered by the Windows Hardware Quality Lab (WHQL). Drivers that earn this certification are more robust and are preferred. Microsoft digitally signs

drivers that pass the WHQL tests so they are recognized natively by Windows Server 2003. Devices covered include:

- Keyboard
- Hard disk controller
- Multimedia device
- Video display
- Modem
- Mouse
- Network adapters
- Printer
- SCSI adapter
- Smart card reader

The system files provided with Windows Server 2003 have a Microsoft digital signature, which indicates that the files are original, unaltered system files, and they have been approved by Microsoft for use with Windows Server 2003.

All drivers included with Windows Server 2003 are digitally signed by Microsoft. You can verify that third-party drivers have met the WHQL standards and that they have not been modified since they were tested. To ensure that device drivers are compatible with Windows Server 2003, look for vendors offering drivers signed by Microsoft.

Checking for Digital Signatures

Windows Server 2003 includes the File Signature Verification tool and signature checking to identify files that have been signed.

With the File Signature Verification tool, you can determines whether a file is signed and do the following:

- View the certificates of signed files to ensure that a file has not been tampered with after being certified.
- Search for signed files in a specific location.
- Search for unsigned files in a specific location.

To run the File Signature Verification tool, click **Start**, click **Run**, and then type **sigverif** and click **OK**. The **File Signature Verification** too opens. To customize its behavior, click **Advanced**. The **Advanced File Signature Verification Settings** dialog box provides the following option tabs:

- **Search** enables you to search all drivers or specify the name and location of the driver search.
- **Logging** saves the program's results as a log file. You can provide a file name and determine whether to overwrite or append to an existing file and view the existing log.

The log file, Sigverif.txt, is stored in the %systemroot% folder by default, and records the following information about the files it scans:

- Name
- Modification date
- Version number
- Signed status
- Location

Signature Checking

Signature Checking can be enabled by system administrators to ensure that Windows Server 2003 inspects files for digital signatures whenever drivers are installed.

Signature Checking has three levels:

- **Level 0** disables digital signature checking. The dialog box that identifies a digitally signed driver does not appear, and all drivers are installed whether they are signed or not.
- **Level 1** determines whether the driver has passed WHQL testing. A message appears whenever a user tries to install a driver that fails the signature check.
- **Level 2** blocks installation of a driver that fails the signature check. The user is notified that the driver cannot be installed because it is not digitally signed.

You can activate the Signature Checking feature by using the **Hardware** tab of the **System Properties** dialog box.

Windows Server 2003 Minimum System Requirements

System Requirements by Version

Requirement	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition
Minimum CPU Speed	133 MHz	§ 133 MHz for x86-based computers § 733 MHz for Itanium-based computers[1]	§ 400 MHz for x86-based computers § 733 MHz for Itanium-based computers[1]	133 MHz
Recommended CPU Speed	550 MHz	733 MHz	733 MHz	550 MHz
Minimum RAM	128 MB	128 MB	512 MB	128 MB
Recommended Minimum RAM	256 MB	256 MB	1 GB	256 MB
Maximum RAM	4 GB	§ 32 GB for x86-based computers § 64 GB for Itanium-based computers[1]	§ 64 GB for x86-based computers § 512 GB for Itanium-based computers[1]	2 GB
Multiprocessor Support[2]	Up to 4	Up to 8	§ Minimum 8 required § Maximum 64	Up to 2
Disk Space for Setup	1.5 GB	§ 1.5 GB for x86-based computers § 2.0 GB for Itanium-based computers[1]	§ 1.5 GB for x86-based computers § 2.0 GB for Itanium-based computers[1]	1.5 GB

[1] **Important:** The 64-bit versions of Windows Server 2003, Enterprise Edition, and Windows Server 2003, Datacenter Edition, are compatible only with 64-bit Intel Itanium-based systems and cannot be successfully installed on 32-bit systems.

[2] Windows Server 2003 may not be able to use multiple processors with some Intel Pentium Pro or Pentium II Processors. For more information, see Microsoft Knowledge Base Article 319091.

Additional disk space is recommended for domain controllers to support the Active Directory database and log files. Use the following guidelines to determine how much disk space to allocate for an Active Directory installation:

- On the drive that will contain the Active Directory database template, NTDS.dit, provide available space equal to 10 percent of the existing database size, or at least 250 MB.
- On the drive containing the Active Directory ESENT transaction log files, provide at least 50 MB of available space.
- For optimum performance, store the Active Directory database, Active Directory log files, and Windows Server 2003 operating system on separate physical hard disks.
- If you plann to install additional services on the domain controllers, allocate sufficient processor, memory, and disk resources. For more information about domain controller capacity planning, see the "Planning for Domain Controller Capacity" section of the Windows Server 2003 Deployment Guide available from on the TechNet Web site at http://www.microsoft.com/technet/prodtechnol/WindowsNetServer/Evaluate/CPP/Reskit/ADSec/.
- Use a hardware assessment table to document hardware and software information for each domain controller. For a sample worksheet to assist you in documenting hardware information, see the "Hardware Assessment" document in the Windows Server 2003 Deployment Kit.

Assessing and Documenting Server Upgrade Order

Your upgrade plan should identify and document the domain controllers in the existing Windows NT 4.0 domain. Include in the documentation the role that each domain controller holds in the domain, and the services that each domain controller provides. Be sure to identify servers that provide Remote Access Service (RAS) and LAN Manager Replication (LMRepl), because upgrading to Windows Server 2003 affects these services.

For a worksheet to use in documenting servers and services, see the "Domain Controllers and Services Documentation" section in the Windows Server 2003 Deployment Kit.

Analyze the servers to determine the order in which the various servers should be upgraded. This analysis should take the following into consideration:

- Number of servers to be upgraded or decommissioned.
- Applications running on the various servers.
- Services running on the various servers.

Number of Servers

Calculate how many servers will be involved in the upgrade. Determine an upgrade priority for each server. For example, if the plan is to perform an in-place domain upgrade, the Windows NT 4.0 primary domain controller (PDC) is near the top of the list, because it must be upgraded before the domain can be upgraded to Active Directory.

Another approach might be starting with member servers. Windows NT 4.0 member servers can be upgraded to Windows Server 2003 prior to upgrading to Active Directory. This approach enables administrators to experience success while taking advantage of the new features of Windows Server 2003, such as the Volume Shadow Copy Service.

Make sure to document which of the servers will be decommissioned. Some Windows NT 4.0 servers may be running on old hardware. Determine which computers can be retired and plan for their services and applications to be rolled into other servers or replaced by new equipment.

Applications on Servers

Determine the critical company applications and corresponding servers, and then assign priorities to these servers. For example, if a parallel upgrade has been chosen, perhaps it would make sense to first upgrade a server with a lightly used application into the new parallel Windows Server 2003 Active Directory domain. The knowledge gained from this first upgrade and each corresponding upgrade helps to make the upgrade of other servers smoother. For more information about determining application compatibility, see Assessing Application Compatibility later in this guide.

Services on Servers

Prioritize the services running on the servers. A detailed analysis of Windows services should be performed. First, make a list of all services and make notes regarding their impact on the user community. Planning the order of services to upgrade is helpful in determining the overall server upgrade order. The following services should be considered:

- Dynamic Host Configuration Protocol (DHCP)
- Windows Internet Name Service (WINS)
- Terminal Services
- File and Print
- Web

Server Upgrade Checklists

The following checklists can be helpful in creating a well-formulated upgrade plan that includes a hardware analysis and evaluates the appropriate server migration order. For more information about applications compatibility issues, see Assessing Application Compatibility later in this document.

Windows NT Server 4.0 to Windows Server 2003 Checklists

Assess and Document Existing Environment Phase	
Do initial tasks:	
☐	Determine supported software upgrades for Windows NT 4.0 servers
☐	Identify computers that can be upgraded
☐	Identify computers to decommission
Document the existing domain structure and domain controller assignments:	
☐	Topology
☐	Network connections
☐	Servers in the domain
☐	Services being provided
☐	Members of the Domain Administrator global group
☐	Number of users in the domain
☐	Workstation operating systems
☐	Any other resources provided in the domain such as printer service or fax service
Create a diagram of the existing Windows NT 4.0 domain. Include the following in the diagram:	
☐	Domain name
☐	Names of servers in the domain
☐	Number of domain controllers in the domain
☐	Trust relationships that the domain shares with other domains
Document how the existing domain controllers are currently assigned, including items such as:	
☐	Computer names
☐	Network information such as IP addresses and subnet masks
☐	Services that are provided
Document the planned Windows Server 2003 network structure, including:	

☐	Domain structure
☐	Intended post-upgrade operations master roles
☐	Order in which domain controllers will be upgraded
☐	Domain Name System (DNS) infrastructure and namespace
☐	Structure of the Windows Server 2003 forest
☐	Relationship of the Windows Server 2003 domains to existing Windows NT 4.0 domains
☐	Relationship of the Windows Server 2003 forest to other forests

Planning the Upgrade Phase	
Determine the order in which to upgrade domains:	
☐	Determine the order in which to upgrade account domains
☐	Determine the order in which to upgrade resource domains
☐	Determine the order in which to upgrade domain objects
Identify service and client compatibility problems:	
☐	Ensure that Windows NT 4.0 Server applications are compatible to run on Windows Server 2003
☐	Ensure RAS compatibility
☐	Ensure Windows 2000 and Windows XP client compatibility
Develop a test plan that verifies that a user:	
☐	Is able to log on
☐	Can access files for which user has permissions
☐	Can access files for which user has user group-membership permission
☐	Cannot access files for which user does not have group-membership permission
☐	Is able to access e-mail resources (if applicable)
Develop a test plan that verifies Windows NT 4.0 domain and Windows Server 2003 Active Directory functionality:	
☐	Verify that the existing Windows NT 4.0 Domain is functioning and replicating between controllers properly
☐	Verify several aspects of the Active Directory configuration with Windows Server 2003 tools
☐	Verify that Active Directory is functioning properly
Develop a recovery plan of the steps needed for recovery of the domain to its original state, including:	
☐	Remove any Windows Server 2003 domain controllers from the domain

☐	Restore network connectivity to the designated backup domain controller (BDC) in the domain
☐	Promote the designated BDC to the PDC
☐	Synchronize all Windows NT 4.0 domain controllers
☐	Test Windows NT 4.0 server operations and domain validation
☐	Document the reasons for the unsuccessful domain upgrade and communicate them to the project team
☐	Restart the planning process for the domain upgrade
☐	Estimated time before recovery must take place
☐	Team review and sign-off

Performing Pre-Upgrade Tasks and Procedures Phase	
Do initial tasks:	
☐	Introduce a Windows Server 2003-based member server
☐	Review the Windows Server 2003 interim functional level documentation
☐	Relocate the LMRepl file replication service
Help protect domain data:	
☐	Back up the PDC and at least one BDC
☐	Synchronize a BDC with the PDC, then remove the BDC from the network
☐	Fully back up any services running on domain controllers
Ensure the following before enabling the Windows NT 4.0 environment change freeze:	
☐	All updates to the Windows NT 4.0 domain are complete and have fully replicated
☐	The Windows NT 4.0 domain administrator global group is configured properly
☐	A BDC has been synchronized and taken offline for recovery purposes
☐	Execute user and Windows NT 4.0 domain test plans

Upgrading Domains from Windows NT 4.0 to Windows Server 2003 Phase	
Initial tasks:	
☐	Configure DNS on the PDC
☐	Upgrade the Windows NT 4.0 PDC
Configure the system to help protect against a PDC Locator overload:	
☐	Emulating a Windows NT 4.0 domain controller

☐	Neutralize Windows NT 4.0 emulation
☐	Synchronize file replication services
Execute user and Active Directory test plans	
☐	Execute User and Active Directory test plans
Complete post-upgrade tasks:	
☐	Add additional domain controllers to the Windows Server 2003 domain
☐	Repeat upgrade steps to upgrade remaining Windows NT 4.0 domains
☐	Consolidate accounts and domains where appropriate
☐	Raise forest and domain functional levels (if desired)
☐	Use DNS application directory partitions
Complete the upgrade process:	
☐	Redeploy the rollback server (if appropriate)
☐	Review, update, and document the domain and forest architecture
☐	Review operating procedures and administrative tasks
☐	Remove the FRS script from the domain controller scheduled to provide the daily script export
☐	Execute final user and Active Directory test plans

Assessing Application Compatibility

When planning an upgrade, questions arise about an application's ability to run on a new version of an operating system. To help simplify this process, Windows Server 2003 provides a tool that can detect application compatibility issues so that they can be fixed before upgrading. The Application Compatibility Toolkit (ACT) provides several tools that help both system professionals and developers prepare and move to Windows Server 2003. With this toolkit, you can inventory, test, resolve, deploy, and debug an existing application that you want to run on Windows Server 2003.

ACT 3.0 also provides tools to create installation patches for applications. Patches for known issues with many applications already exist and are available with ACT. This section provides an introduction to working with ACT. For more information, refer to the documentation provided with the toolkit. See also Using the Application Compatibility Toolkit on the Windows Server 2003 Web site.

About ACT 3.0

ACT 3.0 provides three key tools:

- Application Compatibility Analyzer 1.0
- Windows Application Verifier 2.5
- Compatibility Administrator 3.0

The Application Compatibility Analyzer includes a client-side Collector (Collector.exe), Merger (Merger.exe), and Analyzer (Analyzer.exe). Collector allows information to be collected about the computers in an organization and the software that is installed. Analyzer helps to evaluate the inventory of software gathered by Collector. Merger combines the various collected log files into a database file. By default, Merger enters the data into a Microsoft Access database file (.mdb), but the logs can also be sent to a SQL Server database. The collected information can then be compared to an online database from Microsoft of known compatibility issues for the specified applications. This database, in many cases, provides the deployment packages needed to address certain incompatibilities so than an application can run on Windows Server 2003.

In general, after installing ACT 3.0, you use its tools in the following order:

1. Run Collector.
2. Run Analyzer.
3. Run Application Verifier.
4. Run Compatibility Administrator.

Installing ACT 3.0

To download and install ACT 3.0, do the following:

1. Download the tool kit from the Windows Application Compatibility Toolkit 3.0 page at the Microsoft Download Center Web site

(http://www.microsoft.com/downloads/details.aspx?FamilyID=7fc46855-b8a4-46cd-a236-3159970fde94).

2. Double-click **Act30pkg.exe**.

3. Follow the on-screen instructions.

Many of the tools in ACT 3.0 run only on Windows Server 2003, Windows XP, or Windows 2000. However, Collector, a client-side tool, runs on all Windows 95 and later operating systems, as the following table shows.

Supported Operating Systems for ACT 3.0 and Collector

Tool	Supported Operating Systems
ACT 3.0	§ Windows Server 2003 § Windows XP § Windows 2000 Professional § Windows 2000 Server
Collector (Collector.exe)	§ Windows Server 2003 § Windows XP § Windows 2000 Professional § Windows 2000 Server § Windows NT 4.0 Workstation § Windows NT 4.0 Server § Windows 95 § Windows 98 § Windows Millennium Edition (Windows Me)

Making an Inventory with Collector

Obtaining an inventory of all the applications running on a system can be performed by a simple command-line tool, Collector, which is included with ACT 3.0. Collector is a client-side tool that can be deployed to computers by copying the Collector.exe file to a floppy disk and installing on the client computer, or through more advanced mechanisms like adding it to a logon script or using Microsoft Systems Management Server (SMS). The goal of running Collector is to obtain a complete inventory of all applications in the enterprise that need to be supported on Windows Server 2003.

Running Collector

The data generated by Collector is stored in compressed .cab files by default or uncompressed XML files if specified. The location of these files is controlled by using the command-line switches when running the tool. It's a good idea to create a network share first to store the inventory files, and then run Collector on all the computers planned for upgrade. By default, if a location to store the inventory files is not specified, the inventory files appear on the desktop of the user who invoked Collector. The files are uniquely identifiable, so there is no need to worry about one computer overwriting the data collected for another.

The Collector.exe file is located in the following folder:

```
Program Files\Microsoft Windows Application Compatibility
Toolkit\Applications\Microsoft Application Compatibility Analyzer\Collector
```

For instructions about running the tool, type **collector /?**, which displays information similar to the following:

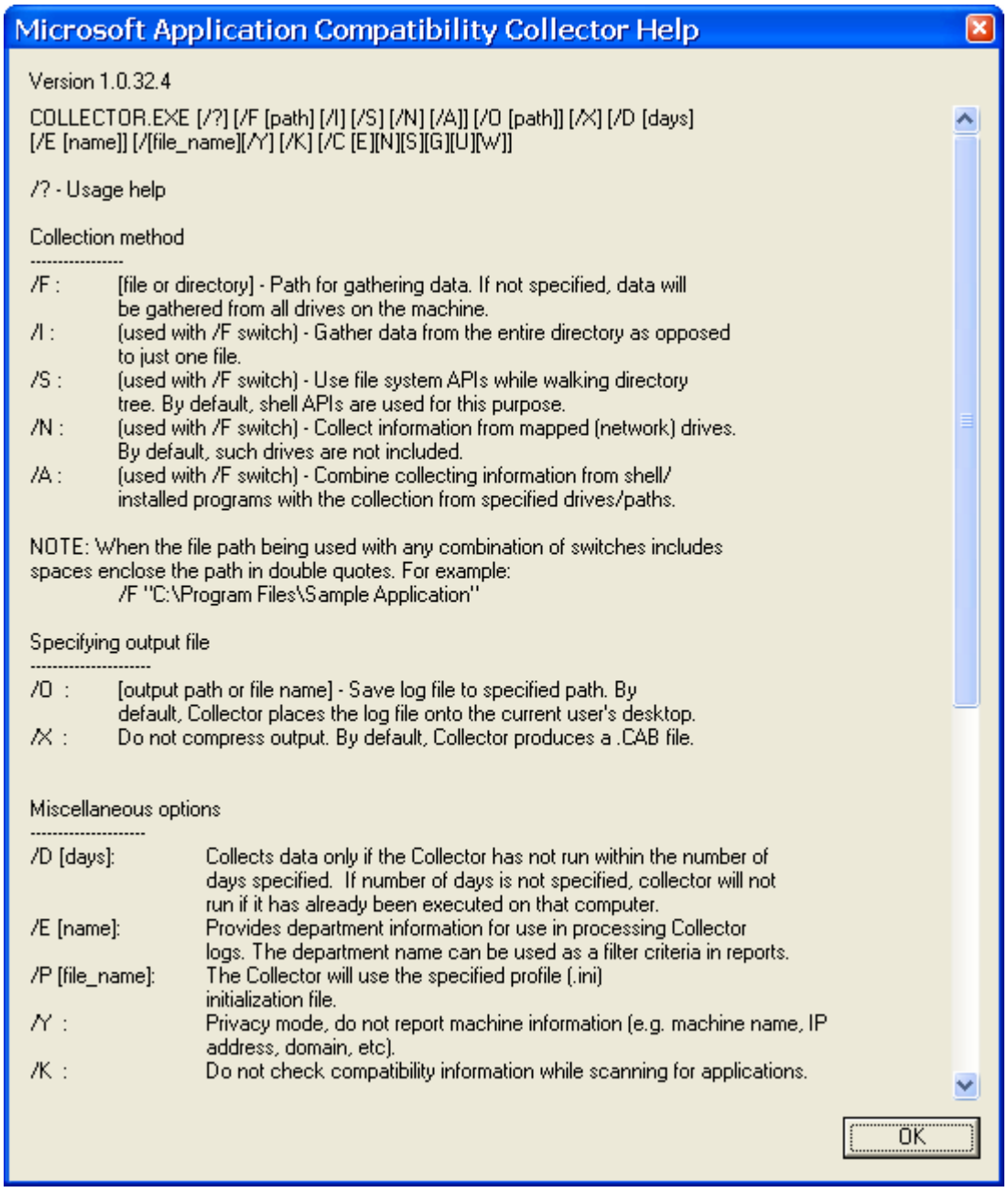

Microsoft Application Compatibility Collector Help
Version 1.0.32.4
COLLECTOR.EXE [/?] [/F [path] [/I] [/S] [/N] [/A]] [/O [path]] [/X] [/D [days]
[/E [name]] [/[file_name][/Y] [/K] [/C [E][N][S][G][U][W]]
/? - Usage help
Collection method
/F : [file or directory] - Path for gathering data. If not specified, data will be gathered from all drives on the machine.
/I : (used with /F switch) - Gather data from the entire directory as opposed to just one file.
/S : (used with /F switch) - Use file system APIs while walking directory tree. By default, shell APIs are used for this purpose.
/N : (used with /F switch) - Collect information from mapped (network) drives. By default, such drives are not included.
/A : (used with /F switch) - Combine collecting information from shell/ installed programs with the collection from specified drives/paths.
NOTE: When the file path being used with any combination of switches includes spaces enclose the path in double quotes. For example:
/F "C:\Program Files\Sample Application"
Specifying output file
/O : [output path or file name] - Save log file to specified path. By default, Collector places the log file onto the current user's desktop.
/X : Do not compress output. By default, Collector produces a .CAB file.
Miscellaneous options
/D [days]: Collects data only if the Collector has not run within the number of days specified. If number of days is not specified, collector will not run if it has already been executed on that computer.
/E [name]: Provides department information for use in processing Collector logs. The department name can be used as a filter criteria in reports.
/P [file_name]: The Collector will use the specified profile (.ini) initialization file.
/Y : Privacy mode, do not report machine information (e.g. machine name, IP address, domain, etc).
/K : Do not check compatibility information while scanning for applications.
OK

Figure 1. Instructions for using Collector.exe

Sample Application Inventory with Collector

The following example illustrates how Collector and Application Compatibility Analyzer can be used in a network environment.

A company is preparing to deploy Windows XP Professional to all desktop computers. The organization is divided among three physical locations connected by high-speed data connections. The organization uses the Active Directory service within a single domain, and has created an organizational unit (OU) for each physical location (HQ, East, and West).

On Server1, the IT department creates a shared folder for storing all log files generated by Collector, with the Universal Naming Convention (UNC) path \\Server1\Analyzer, and another shared folder for storing the Collector executable, with the path \\Server1\Collector. The IT department decides to use a logon script assigned through Active Directory to distribute and run Collector. Because the three physical locations are represented by three separate OUs within the domain, the organization decides to gather data by OU. To accomplish this, the IT department adds the following lines to the logon script:

```
Copy \\server1\collector\collector.exe c:\
C:\collector.exe /O \\server1\analyzer /N /E HQ /CW
```

The first line of code copies Collector executable from the shared folder on Server1 to drive C on the client computer. The second line of the code instructs Collector to do the following:

- Send log file output to the shared folder on Server1 that is specified for storing logs (using the /O switch).
- Scan network drives that might be mapped (using the /N switch).
- Mark the data with an **HQ** designation for the HQ OU (using the /E switch).
- Wait five minutes before starting the collection.

The IT department can include similar lines for the logon scripts in the East and West OUs, with the exception that the /E switch would define the OU name in each case

What Collector Does

Collector inspects all the applications installed on a computer and builds an inventory file in either a compressed .cab format or an uncompressed .xml format. This information is then used by Analyzer. The data can be gathered easily and quickly throughout the network when deployed through mechanisms such as logon scripts. The goal of Collector is to provide a quick and easy way to gather the inventory of systems running in the enterprise. This data is then used to find, determine, and fix compatibility issues.

Note Make sure to install and inventory applications that you intend to run in the new environment but that may not yet be running, so you can also verify compatibility with those new applications.

A sample file collected by Collector includes XML and looks similar to the following:

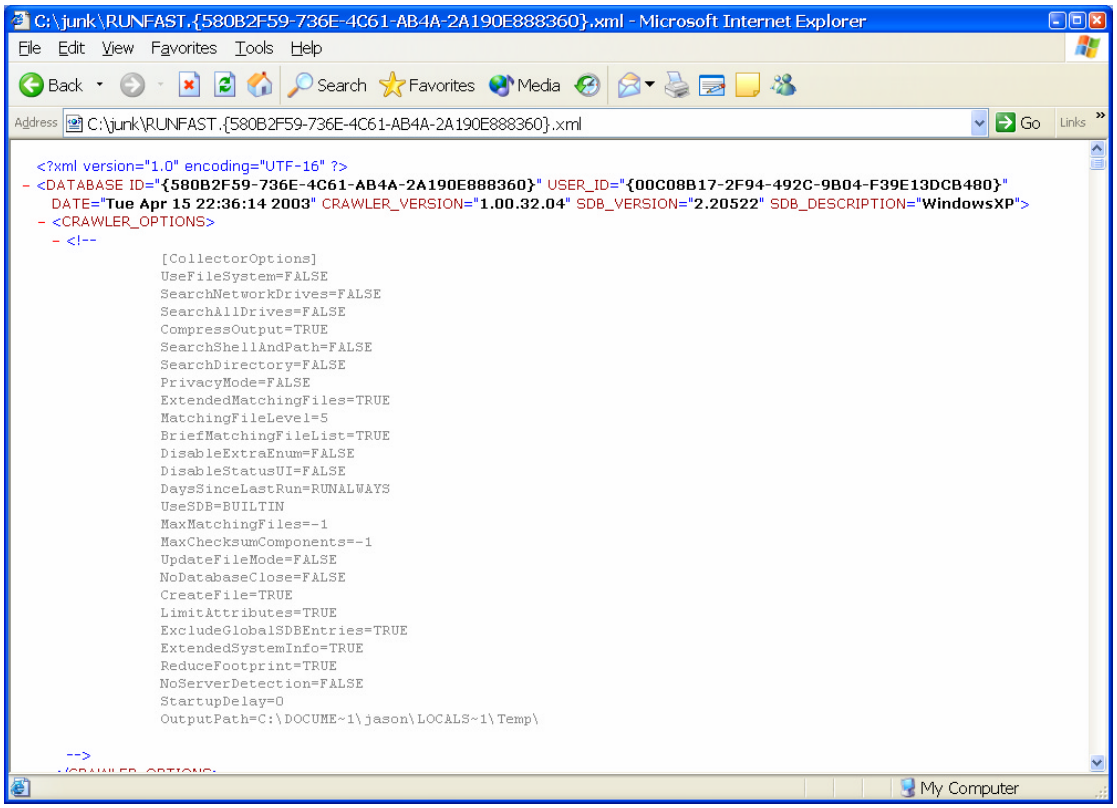


Figure 2. XML file generated by Collector

Using Analyzer 1.0

Analyzer 1.0 consists of two pieces, Collector for gathering data and the Analyzer for processing that data. After you've run Collector, you use Analyzer to process the collected data.

Running Analyzer

Analyzer is used to perform an analysis and reporting of all the data gathered by Collector. Before running the Analyzer, make sure Collector has run and generated log files for the Analyzer to process. Then follow the steps to start analyzing software inventory.

After starting the Analyzer, the following screen appears:

Microsoft Application Compatibility Analyzer (1.0)
Back
Forward
Home
Update
Help
Microsoft
Windows
Application Compatibility Analyzer
Microsoft
Resources
About Microsoft Application Compatibility Analyzer
Application Compatibility Toolkit
Application Experience Website
Welcome to the Microsoft Application Compatibility Analyzer
The Microsoft Application Compatibility Analyzer tool collects application information from your organization's computers, along with identifying machine information. It can be used to inventory your organization's applications providing reports that can be updated, printed, or exported. Additionally, the Analyzer can check for the compatibility status of your applications by querying an online database at Microsoft. For more information on using the Analyzer, please refer to the help pages.
If you prefer to only analyze this local computer click here. Otherwise, click on the "Start using the Analyzer" link below to begin analysis on the computers in your organization.
Start using the Analyzer

Figure 3. Analyzer 1.0

Creating an Analyzer Database

The first time the Analyzer runs, it prompts the user to create a new database or open an existing database. There is an option for creating an Access database or a SQL Server database. If a SQL Server database is chosen, SQL Server must be installed and running. If SQL Server is not available, choose the Access option to have the tool create an Access database.

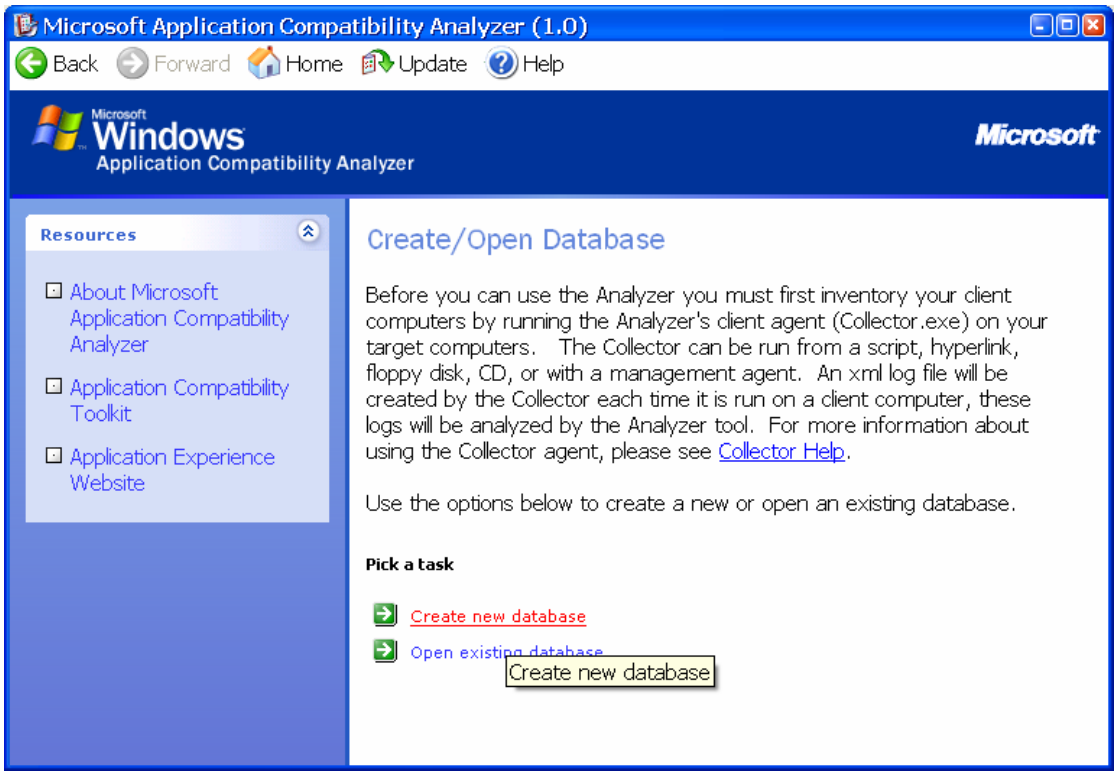

Microsoft Application Compatibility Analyzer (1.0)
Back
Forward
Home
Update
Help
Microsoft
Windows
Application Compatibility Analyzer
Microsoft
Resources
About Microsoft Application Compatibility Analyzer
Application Compatibility Toolkit
Application Experience Website
Create/Open Database
Before you can use the Analyzer you must first inventory your client computers by running the Analyzer's client agent (Collector.exe) on your target computers. The Collector can be run from a script, hyperlink, floppy disk, CD, or with a management agent. An xml log file will be created by the Collector each time it is run on a client computer, these logs will be analyzed by the Analyzer tool. For more information about using the Collector agent, please see Collector Help.
Use the options below to create a new or open an existing database.
Pick a task
Create new database
Open existing database
Create new database

Figure 4. Creating a new database

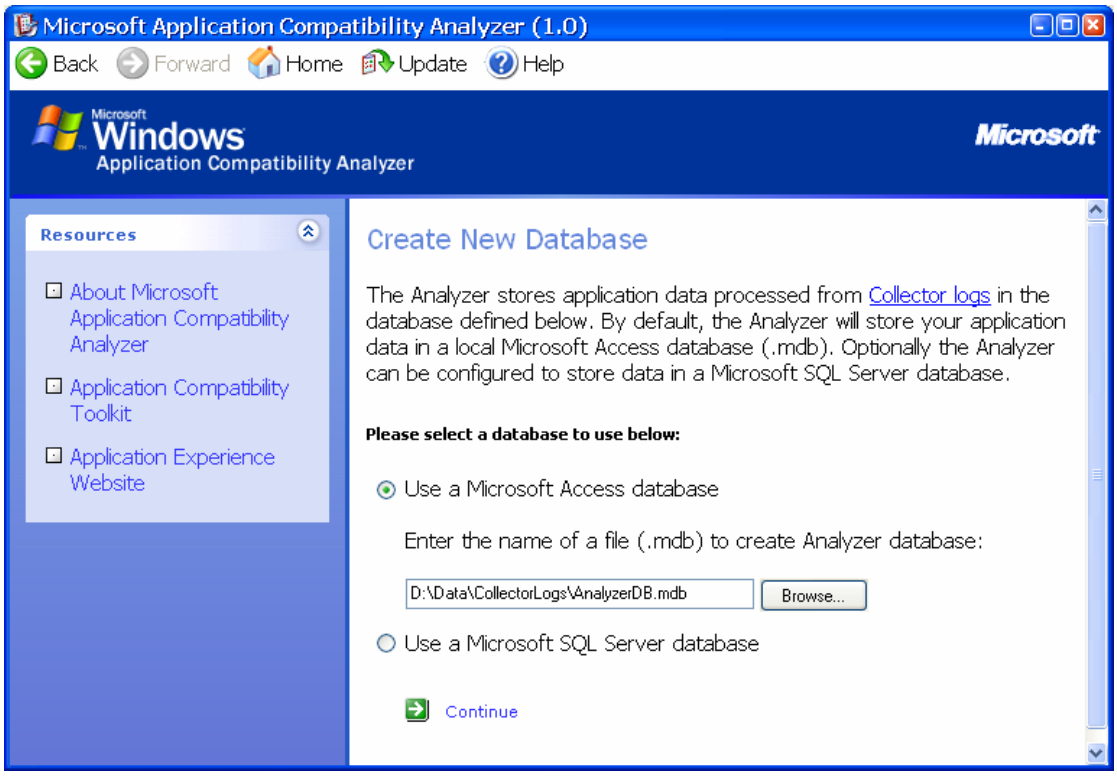

Microsoft Application Compatibility Analyzer (1.0)
Back
Forward
Home
Update
Help
Microsoft
Windows
Application Compatibility Analyzer
Microsoft
Resources
About Microsoft Application Compatibility Analyzer
Application Compatibility Toolkit
Application Experience Website
Create New Database
The Analyzer stores application data processed from Collector logs in the database defined below. By default, the Analyzer will store your application data in a local Microsoft Access database (.mdb). Optionally the Analyzer can be configured to store data in a Microsoft SQL Server database.
Please select a database to use below:
Use a Microsoft Access database
Enter the name of a file (.mdb) to create Analyzer database:
D:\Data\CollectorLogs\AnalyzerDB.mdb
Browse...
Use a Microsoft SQL Server database
Continue

Figure 5. Specifying the database type

Specifying the Collector Logs

After a database has been generated, it is populated with data from the inventory files. The files generated by Collector are considered logs that need to be merged into the database for processing by Analyzer. As the figure below shows, the next step is to locate location the logs (.cab or .xml files) created by Collector.

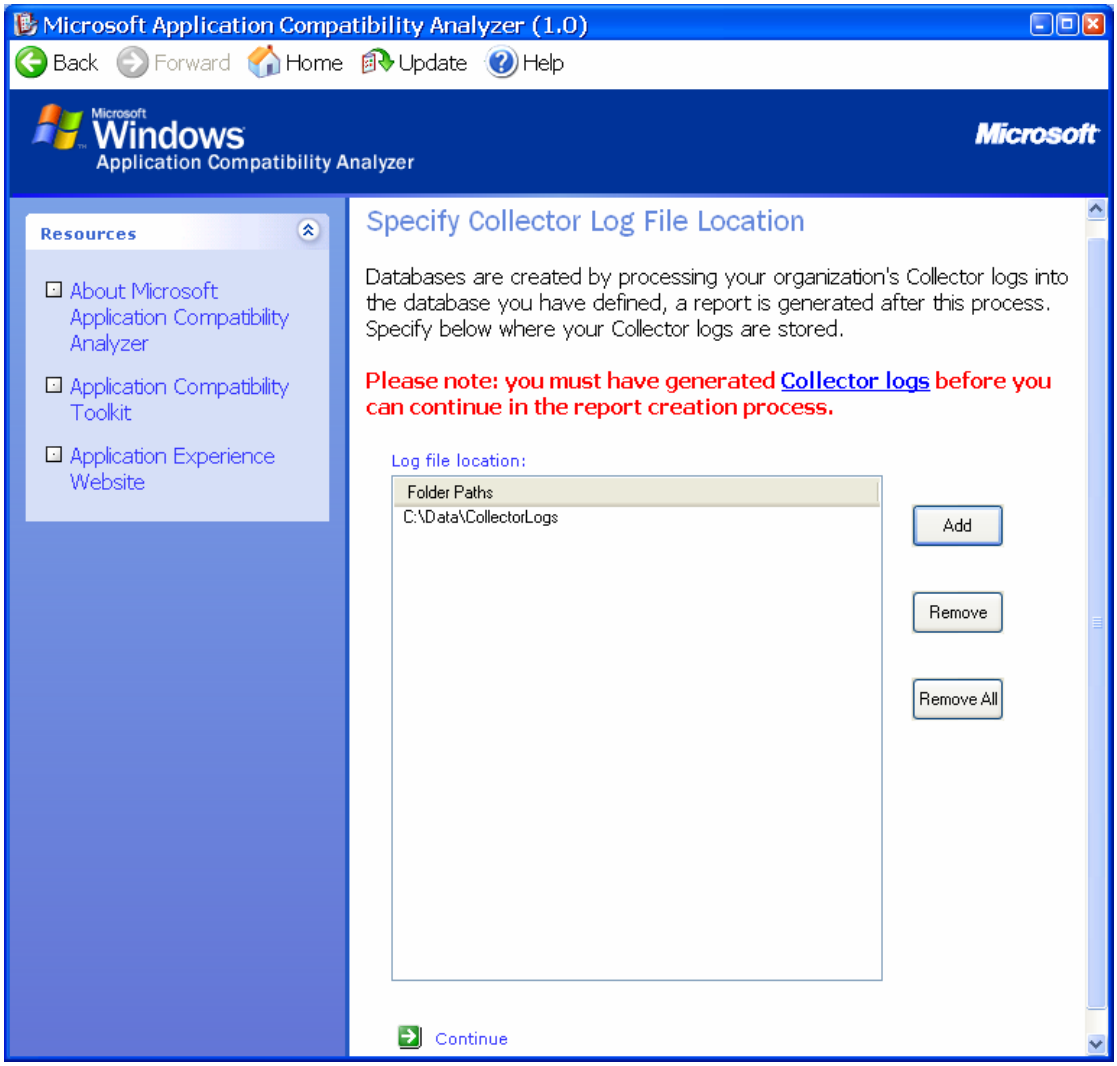


Figure 6. Specifying the Collector logs

Connecting to the Microsoft Compatibility Database

After Analyzer has the data it needs, it provides the option to connect to a Microsoft Compatibility Database. With this option, you can detect additional compatibility information about applications in the inventoried files. To have Analyzer check for known compatibility issues, choose the option to connect to the on-line database as shown below.

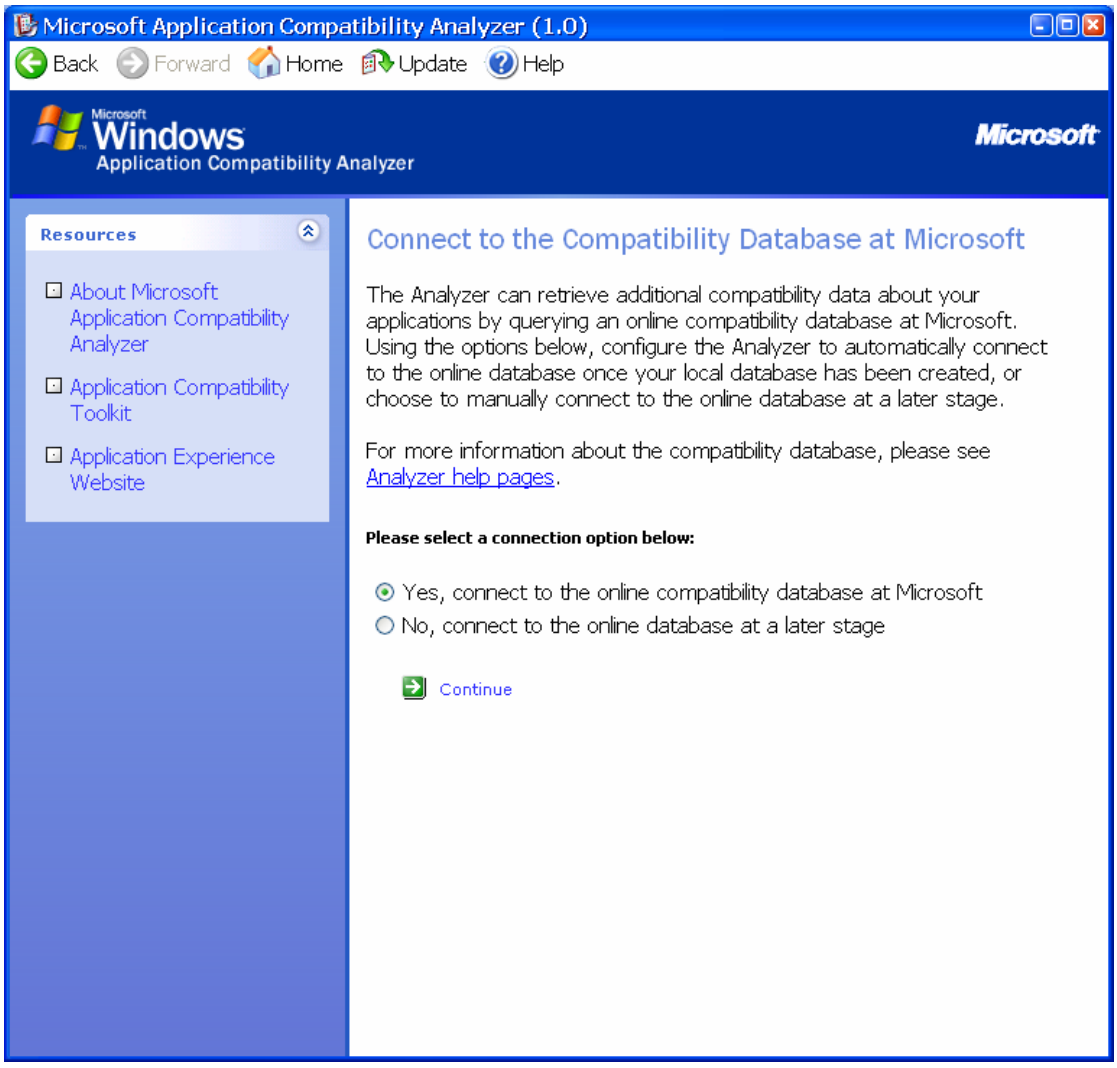

Microsoft Application Compatibility Analyzer (1.0)
Back
Forward
Home
Update
Help
Microsoft
Windows
Application Compatibility Analyzer
Microsoft
Resources
About Microsoft Application Compatibility Analyzer
Application Compatibility Toolkit
Application Experience Website
Connect to the Compatibility Database at Microsoft
The Analyzer can retrieve additional compatibility data about your applications by querying an online compatibility database at Microsoft. Using the options below, configure the Analyzer to automatically connect to the online database once your local database has been created, or choose to manually connect to the online database at a later stage.
For more information about the compatibility database, please see Analyzer help pages.
Please select a connection option below:
Yes, connect to the online compatibility database at Microsoft
No, connect to the online database at a later stage
Continue

Figure 7. Microsoft compatibility database

Next, Analyzer can merge the data into its database so that reports can be run and the data analyzed. Analyzer is invoked, the inventory files are merged into the database, and then the on-line compatibility database is checked. If for any reason the Internet cannot be reached, the compatibility database is not checked. This error is not critical—the compatibility check can be performed later. To ensure success, make sure that the Internet can be reached from the computer running the tool, and then continue. Analyzer displays the files it is merging into the database with a screen similar to the following:

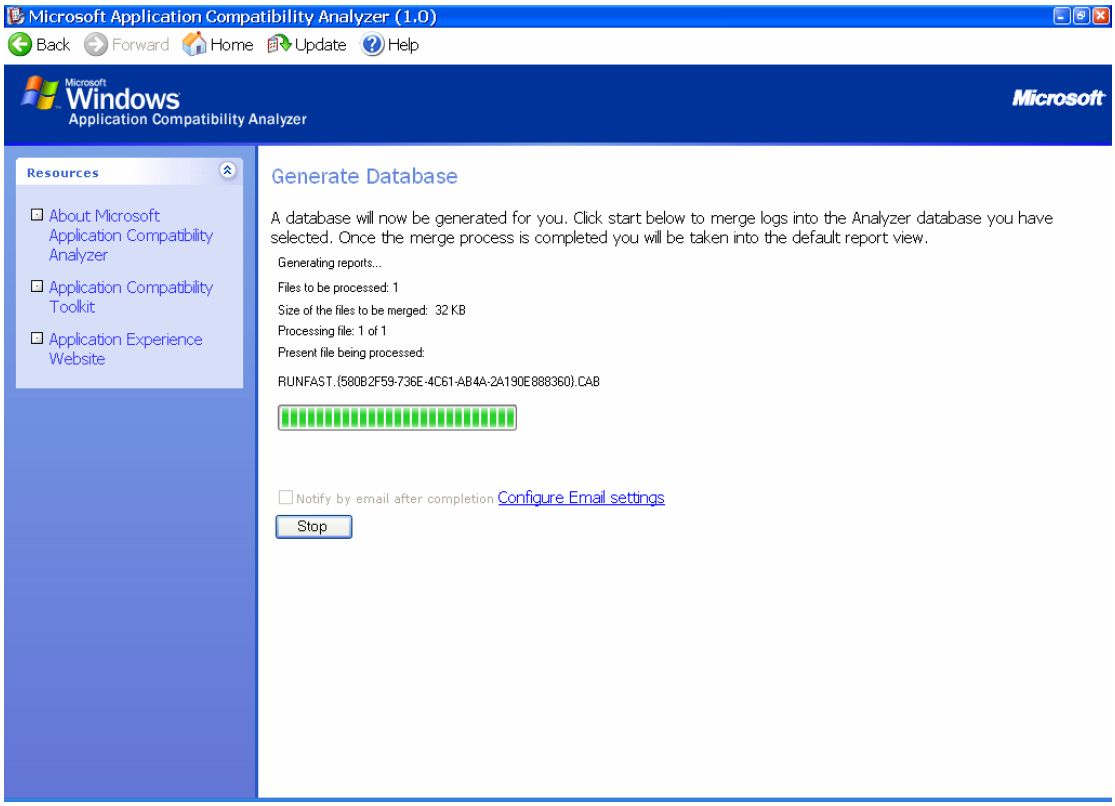

Microsoft Application Compatibility Analyzer (1.0)
Back
Forward
Home
Update
Help
Windows
Application Compatibility Analyzer
Microsoft
Resources
About Microsoft Application Compatibility Analyzer
Application Compatibility Toolkit
Application Experience Website
Generate Database
A database will now be generated for you. Click start below to merge logs into the Analyzer database you have selected. Once the merge process is completed you will be taken into the default report view.
Generating reports...
Files to be processed: 1
Size of the files to be merged: 32 KB
Processing file: 1 of 1
Present file being processed:
RUNFAST.{580B2F59-736E-4C61-AB4A-2A190E888360}.CAB
Notify by email after completion
Configure Email settings
Stop

Figure 8. Database generation and inventory files processed

After the database has been generated and all inventory files have been merged, a report showing all the information that was gathered about the applications deployed in the enterprise appears. This report shows the number of applications that are compatible as well as those that are not compatible and those that are unknown. Many options are provided for filtering, exporting, and reporting on the information important for upgrade.

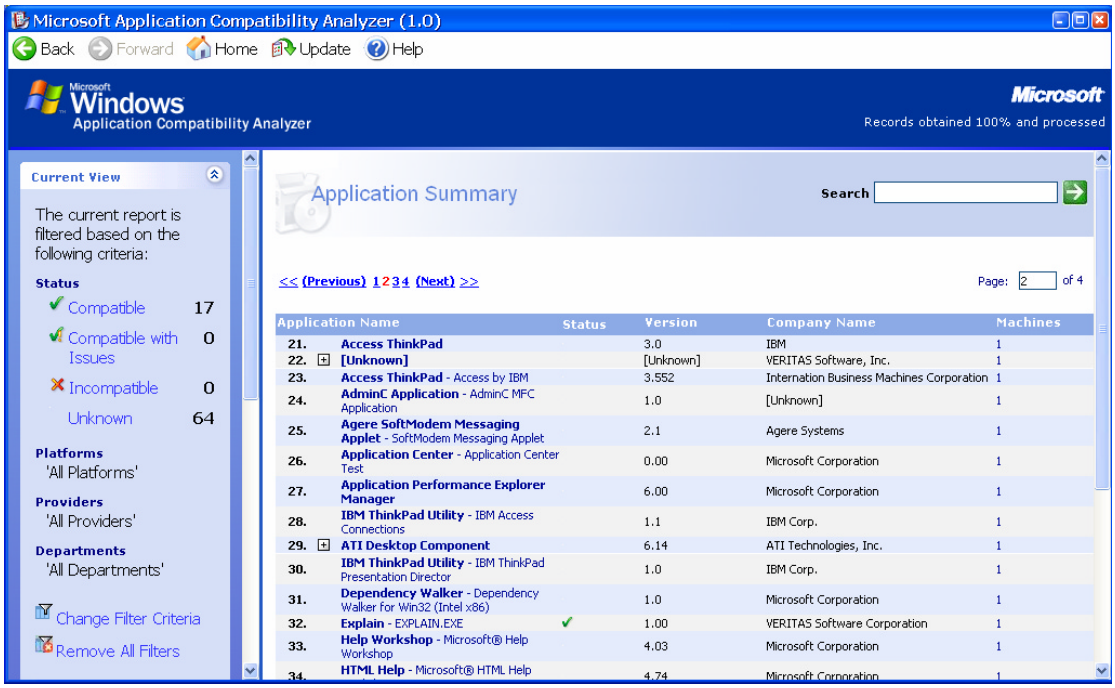

Microsoft Application Compatibility Analyzer (1.0)
Back
Forward
Home
Update
Help
Windows
Application Compatibility Analyzer
Microsoft
Records obtained 100% and processed
Current View
The current report is filtered based on the following criteria:
Status
Compatible 17
Compatible with Issues 0
Incompatible 0
Unknown 64
Platforms
'All Platforms'
Providers
'All Providers'
Departments
'All Departments'
Change Filter Criteria
Remove All Filters
Application Summary
Search
<< (Previous) 1 2 3 4 (Next) >>
Page: 2 of 4
Application Name
Status
Version
Company Name
Machines
21. Access ThinkPad 3.0 IBM 1
22. [Unknown] [Unknown] VERITAS Software, Inc. 1
23. Access ThinkPad - Access by IBM 3.552 Internation Business Machines Corporation 1
24. AdminC Application - AdminC MFC Application 1.0 [Unknown] 1
25. Agere SoftModem Messaging Applet - SoftModem Messaging Applet 2.1 Agere Systems 1
26. Application Center - Application Center Test 0.00 Microsoft Corporation 1
27. Application Performance Explorer Manager 6.00 Microsoft Corporation 1
28. IBM ThinkPad Utility - IBM Access Connections 1.1 IBM Corp. 1
29. ATI Desktop Component 6.14 ATI Technologies, Inc. 1
30. IBM ThinkPad Utility - IBM ThinkPad Presentation Director 1.0 IBM Corp. 1
31. Dependency Walker - Dependency Walker for Win32 (Intel x86) 1.0 Microsoft Corporation 1
32. Explain - EXPLAIN.EXE 1.00 VERITAS Software Corporation 1
33. Help Workshop - Microsoft® Help Workshop 4.03 Microsoft Corporation 1
34. HTML Help - Microsoft® HTML Help 4.74 Microsoft Corporation 1

Figure 9. Application Summary in Analyzer

What's Next?

After an inventory is gathered, the next step is to build a readiness plan. Start by identifying the critical applications you intend to support, verify their compatibility, and obtain available patches from Microsoft. Next, use Application Compatibility Administrator to apply a series of possible fixes to applications. Like Analyzer, Administrator is available as a free download from Microsoft and is part of the ACT 3.0 Toolkit.

For more details on working with the Application Compatibility Administrator, see the documentation for ACT 3.0.

Upgrading Windows NT 4.0 Servers

After application compatibility has been determined, it is time to focus on the steps needed to upgrade Windows NT Server 4.0 computers to Windows Server 2003. This section explains the benefits of upgrading to Windows Server 2003 apart from implementing Active Directory, which is discussed in a later section. Even if Active Directory is not installed, an upgrade to Windows Server 2003 can be a cost-effective decision. Windows Server 2003 provides many benefits, including improved disaster recovery features and performance and scalability, that enable server consolidation.

Many Windows NT 4.0 upgrades to Windows Server 2003 start with individual servers rather than Active Directory. This approach helps administrators become familiar with and take advantage of Windows Server 2003 features without assuming the responsibility of a complete domain upgrade. It is a good idea to start with servers that affect the fewest number of users. That way, staff can implement Windows Server 2003 with little impact to users and become knowledgeable about the operating system before tackling more complicated upgrades that include as Active Directory.

What about servers that are not upgraded? Inevitably, some servers cannot be upgraded. Perhaps the Application Compatibility Toolkit found that an application written internally or by an outside source will not work after an upgrade. It may be some time before that application can be migrated to a new version. Organizations may decide not to wait for one application before starting an upgrade process. However, even in cases like these, Windows Server 2003 can be rolled out for all other Windows NT 4.0 servers. Windows Server 2003 and Active Directory are designed to support backward compatibility with both Windows NT Server 4.0 and Windows 2000 computers. (For details, see the Migrating to Active Directory section later in this guide.)

This section examines the benefits of upgrading stand-alone and member servers even without Active Directory and provides a sample upgrade scenario to demonstrate each step in the process.

Upgrading Windows NT 4.0 Stand-alone Servers

A Windows NT 4.0 stand-alone server is a server that does not participate in a domain. There are many reasons for complete stand-alone servers. One example is a SMTP server sitting in the perimeter network (also known as DMZ, demilitarized zone, and screened subnet). It is not unusual to find this type of server residing in a workgroup as opposed to a domain. Whether a Windows NT 4.0 server is part of a domain or a stand-alone server in a workgroup, it can benefit from an upgrade to Windows Server 2003.

Upgrading Windows NT 4.0 Member Servers

There are a number of reasons to upgrade member servers in a domain to Windows Server 2003. File system management is superior to Windows NT Server 4.0, thanks to improvements in DFS and the addition of the Volume Shadow Copy service, which work together to make file servers highly available and easy to navigate.

As a print server, Windows Server 2003 offers improvements in manageability, reliability, and performance. Print driver management and reliability has been improved with kernel-mode driver blocking, giving administrators control over driver installation on the server.

Windows Server 2003 maintains a high level of backward compatibility with Windows 2000 and Windows NT 4.0 computing environments. Features such as IIS 5.0 isolation mode, a feature of IIS 6.0, ensure compatibility with previous and third-party products. Adding a new server running Windows Server 2003 to an existing Windows NT domain does not necessarily require replacing existing software and infrastructure. The improved performance and management of Windows Server make it an ideal operating system for consolidating existing services.

The following sections describe a few of the enhancements provided by Windows Server 2003. For a more detailed look at these improvements, see Coexistence of Windows Server 2003 and Windows NT 4.0 on the Windows Server 2003 Web site.

DFS

One of the biggest improvements for file servers is DFS, which takes an existing file infrastructure and creates a single, logical view of files stored on multiple servers. This system is entirely transparent to users who have the DFS client on their local computer. The DFS client is built into Windows NT 4.0 and all later Microsoft operating systems. DFS makes files much easier to find, because users do not need to know which server a file is on. DFS also improves scalability, making it easy to add file servers or balance the workload among servers without disrupting users' ability to find and access files.

Windows Server 2003 enhances the reliability of DFS by allowing a single server to host multiple DFS roots, which means DFS can now be clustered for high availability and load balancing. You can also store multiple copies of file shares for redundancy. FRS works with DFS to maintain synchronized copies of data on file shares, so that in the event of a failure, DFS can transparently redirect requests for data to a different server.

For better management on the corporate level, administrators can delegate control of a specific portion of the DFS namespace rather than the entirety. This feature streamlines IT processes and makes the entire infrastructure easier to maintain. DFS is fully integrated with Windows NT 4.0 security. One or more servers running Windows Server 2003 with DFS can help you replace or aggregate your existing file structure into a single hierarchy that is easy to use and maintain.

Volume Shadow Copy Service

Volume Shadow Copy service is a new feature in Windows Server 2003 that enhances data management in two primary ways. First, it allows for the creation of point-in-time copies of data on a volume. Backups can be done online, without stopping server activity, and without the problems of inconsistent data or open files being left out. Backups can also be scheduled to correspond with periods of low network usage.

Volume Shadow Copy service maintains a set of previous versions of files, called shadow copies, which can be used for data recovery when a file is damaged through human error, reducing the frequency of restoring files from backup tapes. Shadow copies are incremental backups that record only the files that have changed since the last backup. As a result, backups take up less

storage space. Volume Shadow Copy service is also supported with a public API, so developers can write applications that use the features of this technology.

The majority of accidental file loss is the result of user error. When a user accidentally overwrites or deletes a file, the result is usually lost time as the user recreates work or contacts a network administrator to restore a file from backup. Users on Windows Server 2003 or the Windows XP Professional operating system can access shadow copies of their files from within Windows Explorer. This ability leads to improved productivity and a reduction in the number of support calls for file restoration. Volume Shadow Copy services for users requires the Volume Shadow Copy service client for Windows XP Professional, found on the Windows Server 2003 installation CD-ROM.

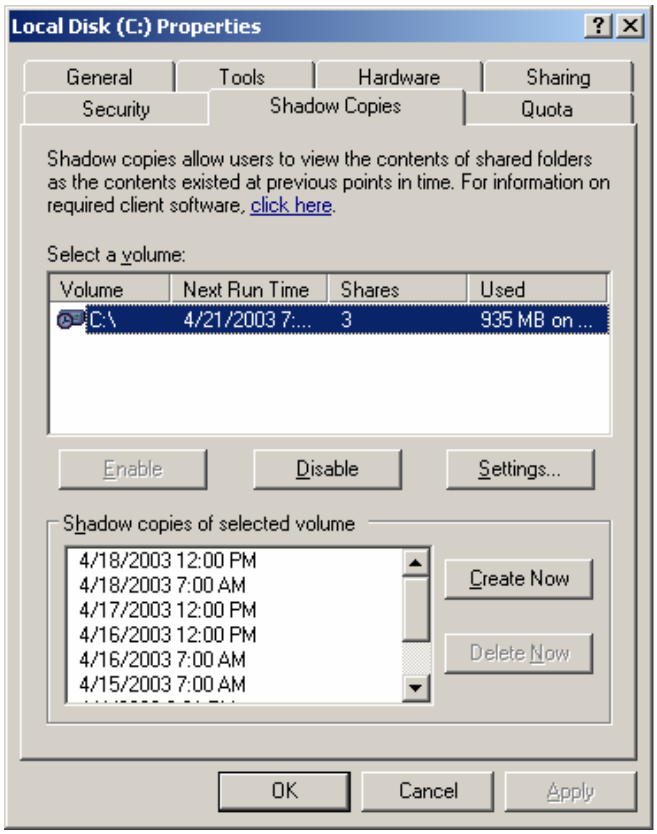


Figure 10. Shadow Copies tab

Virtual Disk Services

Virtual Disk Services enables storage devices from different vendors to interoperate in Windows. VDS has APIs to storage hardware and to management programs that manage the storage hardware. Administrators can discover storage devices from multiple vendors and configure those resources by using a unified interface. Without Virtual Disk Services, each vendor's storage device typically provides its own management interface.

Shadow Copy Restore

After the shadow copy features are enabled on a server or network share, users can find previous versions of files in Windows Explorer by right-clicking a file and selecting **Properties**. To see the **Previous Versions** tab, however, the file must be on a share hosted by a server for which the Volume Shadow Copy service has been enabled.

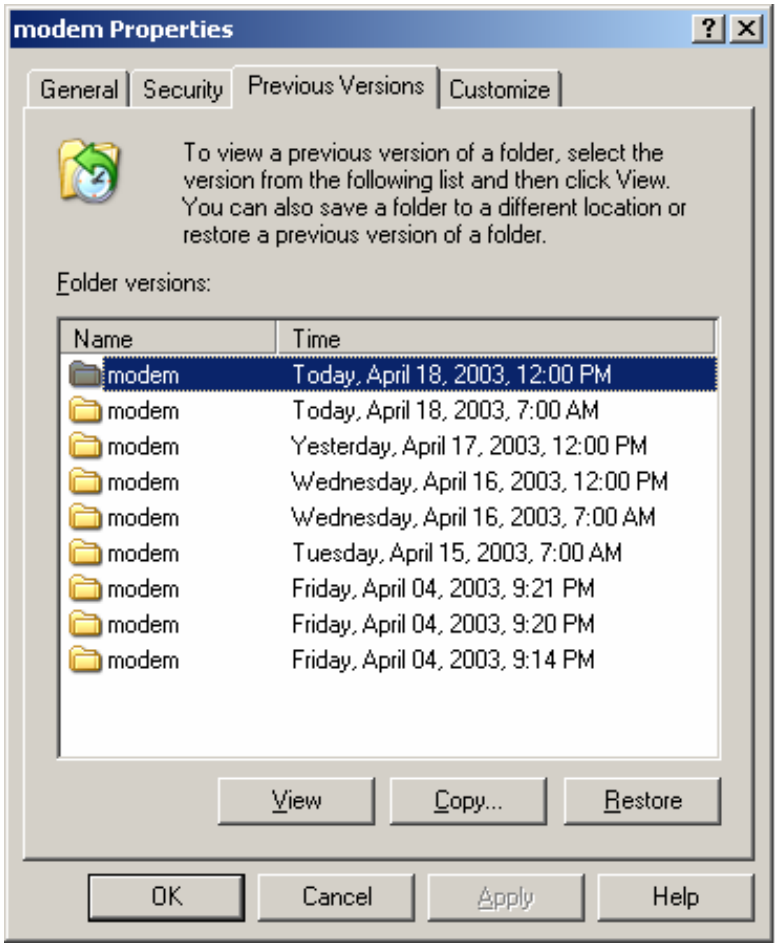

modem Properties
General
Security
Previous Versions
Customize
To view a previous version of a folder, select the version from the following list and then click View. You can also save a folder to a different location or restore a previous version of a folder.
Folder versions:
Name
Time
modem Today, April 18, 2003, 12:00 PM
modem Today, April 18, 2003, 7:00 AM
modem Yesterday, April 17, 2003, 12:00 PM
modem Wednesday, April 16, 2003, 12:00 PM
modem Wednesday, April 16, 2003, 7:00 AM
modem Tuesday, April 15, 2003, 7:00 AM
modem Friday, April 04, 2003, 9:21 PM
modem Friday, April 04, 2003, 9:20 PM
modem Friday, April 04, 2003, 9:14 PM
View
Copy...
Restore
OK
Cancel
Apply
Help

Figure 11. Previous Versions tab

Print Server Improvements

The latest enhancements to Plug and Play, and built-in support for over 3,800 printer drivers, greatly facilitate hardware installation, configuration, and upgrading. Printers can be installed and configured remotely and by using scripts using WMI in Windows Server 2003. In addition, if you are using a print cluster, you can now install drivers on all nodes in the cluster simultaneously.

Administrators have printer scheduling and access controls, enabling them to optimize printer availability and usage. Most printer management functions can now be handled through a command-line interface as well as scripted for automated management. File spooling has been optimized for higher print volume management, a benefit that helps get documents to users faster. Upgrading your print servers to Windows Server 2003 or aggregating your organization's

printers on a Windows Server 2003 print server can greatly reduce the administrative load associated with maintaining a print infrastructure.

Server Consolidation

Many companies are achieving significant savings by consolidating their core services on Windows Server 2003. Consider consolidating core services, such as user logon, DHCP, DNS, and so on if you want to take advantage of the features and performance of Windows Server 2003 while preserving your existing Windows NT 4.0 domain structure. For example, you may want to do this if you need to support earlier systems that cannot be upgraded or if you want to upgrade systems incrementally.

The benefits of a core service consolidation include increased performance, higher availability, reliability, and access to new features and technologies. Windows Server 2003 can provide faster and more efficient logon and networking and name resolution for a Windows NT 4.0 domain. Consolidating services also provides an opportunity for hardware consolidation as redundant servers are eliminated. In addition, a consolidated environment is easier to manage, not only because it is more centralized, but also because Windows Server 2003 offers improved management features.

DNS and DHCP

A Windows Server 2003 domain member server in a Windows NT 4.0 domain can be used to host DNS for the domain. In this way, you can take advantage of the higher reliability and performance of Windows Server 2003 DNS, as well as its security-enhancing features, such as dynamic update and support for Internet Engineering Task Force (IETF) RFC2535 DNS security extensions.

DHCP improves user mobility by making it easier for users to connect to the network wherever they are. It also simplifies IP address management administrators. Windows Server 2003 includes enhanced management tools for DHCP, including automated backup and restore and upgrade of the DHCP database. These tools eliminate many time-consuming tasks that formerly had to be done by hand.

Generally speaking, when using Windows Server 2003 for DNS and DHCP, the main consideration for determining how many servers you require is not server performance, but rather geographical locations and network performance across locations. In many organizations, this reality can mean eliminating the bulk of their existing servers, resulting in hardware savings.

Incremental Upgrade

Core services consolidation has the advantage of being an important incremental step on the way to an upgrade to Windows Server 2003 domains and forests running with Active Directory. Ultimately, many organizations will want to take advantage of the opportunities provided by implementing Active Directory. However, the idea of upgrading to Active Directory can be a challenging proposition. In the mean time, upgrading core services tends to be less complex and enables administrators to start getting comfortable with the new operating system.

An incremental upgrade offers an alternative to the complexity of upgrading your entire infrastructure at once. Core services hosted on Windows Server 2003 are easier to integrate into Active Directory when finally introduced. This ease of integration is particularly true in the case of DNS, because upgrading your DNS servers is a necessary step toward a domain upgrade. Active Directory provides single-logon capability and a central repository for information for your entire infrastructure, features that simplify user management and provide superior access to networked resources.

Sample In-Place Upgrade for a Windows NT PDC

This section is a step-by-step upgrade of a commonly configured Windows NT 4.0 domain controller to Windows Server 2003. The goal is to familiarize you with the upgrade process and errors that may occur.

To make the upgrade more interesting and to see the results, this sample assumes that Exchange Server 5.5 and SQL Server 7.0 (common Windows NT 4.0 applications) are installed on the server. Although it is not common for SQL Server and Exchange Server to be loaded on a domain controller, they are included here for demonstration purposes to show how Windows Server 2003 migrates these applications. For further effect, the sample assumes that the server was purposefully left at Service Pack 4 (SP4).

The configuration of the Windows NT 4 server in this sample is as follows:

- Pentium II 400 MHZ processor
- 128 MB RAM
- 8 GB SCSI hard disk (4-GB C: partition and 4-GB D: partition)
- Adaptec SCSI adapter
- Intel network card
- Kingston network card
- ATI video card
- SCSI CD-ROM drive
- Windows NT 4.0 Server with SP4

The following services and applications are installed in this sample:

- PDC (Security Accounts Manager [SAM] database)
- IIS
- FTP
- Exchange 5.5
- SQL Server 7.0

Checking System Compatibility During an Upgrade

To initiate the upgrade of the operating system on the Windows NT 4.0 PDC, you can use either local or shared media. If you choose local media installation and auto-play is enabled, you can initiate the upgrade by inserting the Windows Server 2003 CD into the PDC. If auto-play is disabled, browse the CD for the **winnt32.exe** command and run it. Using media on a network share, you can initiate the upgrade by connecting to the media share point and running the **winnt32.exe** command.

After inserting the Windows Server 2003 Standard Edition CD into the CD-ROM drive, the Setup program automatically starts and the following screen appears:

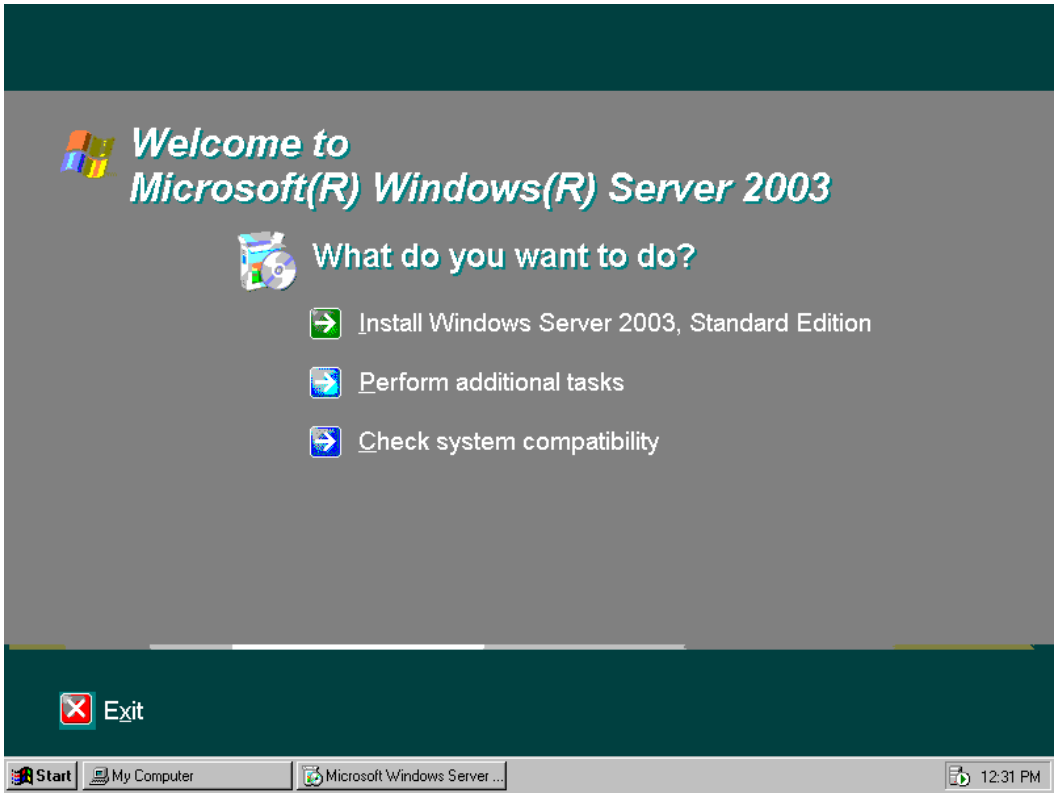


Figure 12. Windows Server 2003 setup screen

This first screen provides the administrator with three options. From here the administrator can choose to install, perform additional tasks such as browsing the CD, or check for system compatibility. At this point it is wise to check system compatibility to get a better picture of what components may be an issue during or after the upgrade.

After choosing Check System Compatibility, a screen similar to the following figure appears.

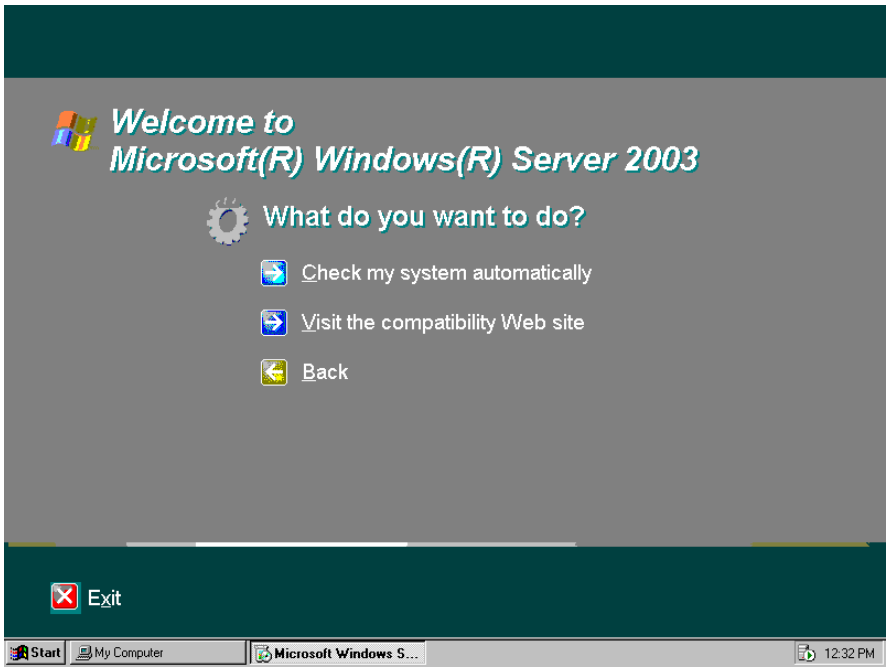


Figure 13.Check System Compatibility screen

At this point the choices are to return to the previous menu, visit the compatibility Web site for more information, or perform an automatic system check. The automatic system check scans a system scanned for potential issues with applications and services running on the server.

When the **Check my system automatically** option is chosen, the following screen appears:

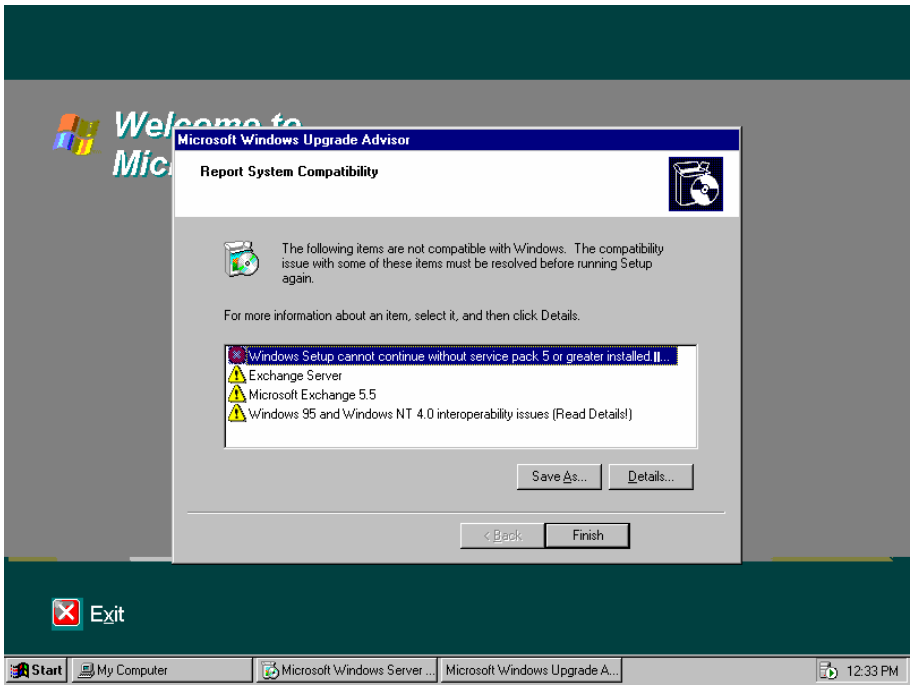

Microsoft Windows Upgrade Advisor
Report System Compatibility
The following items are not compatible with Windows. The compatibility issue with some of these items must be resolved before running Setup again.
For more information about an item, select it, and then click Details.
Windows Setup cannot continue without service pack 5 or greater installed.
Exchange Server
Microsoft Exchange 5.5
Windows 95 and Windows NT 4.0 interoperability issues (Read Details!)
Save As...
Details...
< Back
Finish
Exit
Start
My Computer
Microsoft Windows Server ...
Microsoft Windows Upgrade A...
12:33 PM

Figure 14. System compatibility check with errors

As expected, the report returned some errors. First, it is worth noting that the icon with the red *X* tells an administrator that Setup cannot continue until the problem is resolved. This error is in line with the upgrade prerequisites that require SP5 to be installed before upgrading to Windows Server 2003. The yellow caution icon indicates the Setup can continue, but the highlighted items could have problems. You can select these errors, and then click the **Details** button to display more information similar to the figure below.

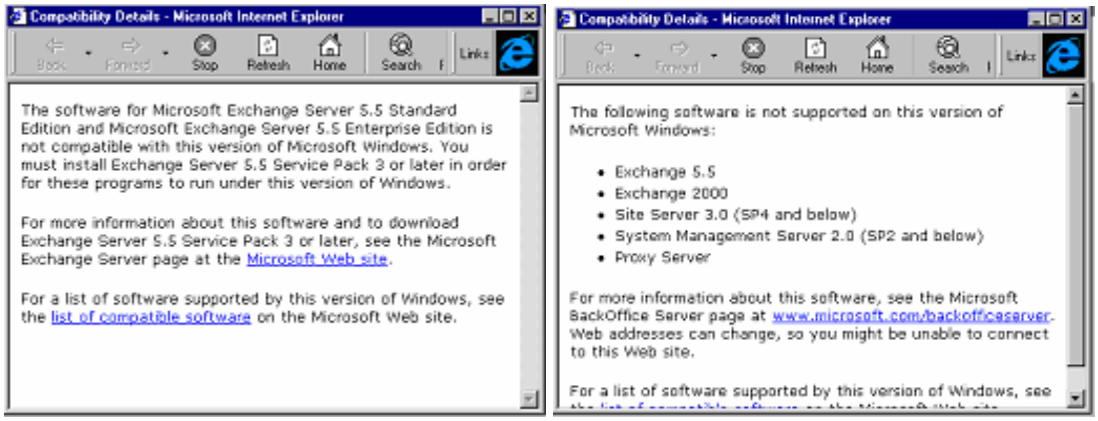

Compatibility Details - Microsoft Internet Explorer
The software for Microsoft Exchange Server 5.5 Standard Edition and Microsoft Exchange Server 5.5 Enterprise Edition is not compatible with this version of Microsoft Windows. You must install Exchange Server 5.5 Service Pack 3 or later in order for these programs to run under this version of Windows.
For more information about this software and to download Exchange Server 5.5 Service Pack 3 or later, see the Microsoft Exchange Server page at the Microsoft Web site.
For a list of software supported by this version of Windows, see the list of compatible software on the Microsoft Web site.
Compatibility Details - Microsoft Internet Explorer
The following software is not supported on this version of Microsoft Windows:
Exchange 5.5
Exchange 2000
Site Server 3.0 (SP4 and below)
System Management Server 2.0 (SP2 and below)
Proxy Server
For more information about this software, see the Microsoft BackOffice Server page at www.microsoft.com/backofficeserver. Web addresses can change, so you might be unable to connect to this Web site.
For a list of software supported by this version of Windows, see

Figure 15. Exchange warning detail dialog boxes

The two screens in Figure 15 give conflicting information about the compatibility of Exchange 5.5 with Windows Server 2003. The error on the right is the most important as it reflects the true status of Exchange 5.5 in Windows Server 2003. Exchange 5.5 and Exchange 2000 are not supported and do not run after a computer is upgraded. The caution and warning messages must be read and thoroughly understood.

The compatibility check also produces a text file that lists the possible problems. Click **Save As**, type a file name, and then view the results of the compatibility check. For a sample log file with the results of the compatibility check for this sample in-place upgrade, see Appendix B: Sample Log File from Compatibility Check.

Starting the Upgrade

After resolving the issues uncovered by the compatibility check, it is time to start the upgrade. After choosing Install Windows Server 2003, the following screen appears:

Microsoft
Windows
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Installation will complete in 60-90 minutes.
To cancel Setup, press the ESC key.
Windows Setup
Welcome to Windows Setup
Which type of installation do you want to perform?
Installation Type:
Upgrade (Recommended)
Upgrade (Recommended)
New Installation (Advanced)
current version of Windows.
Upgrading preserves your installed programs, data files, and existing computer settings.
During Setup, it is normal for your screen to go blank for a few seconds and for the computer to restart itself several times.
< Back
Next >
Cancel

Figure 16. Setup screen with option to upgrade or perform new installation

An administrator can choose a new installation or to upgrade the existing operating system. In this case, the upgrade option is selected, and the following screen appears, where an administrator can download the latest setup files or use the existing setup files from the CD.

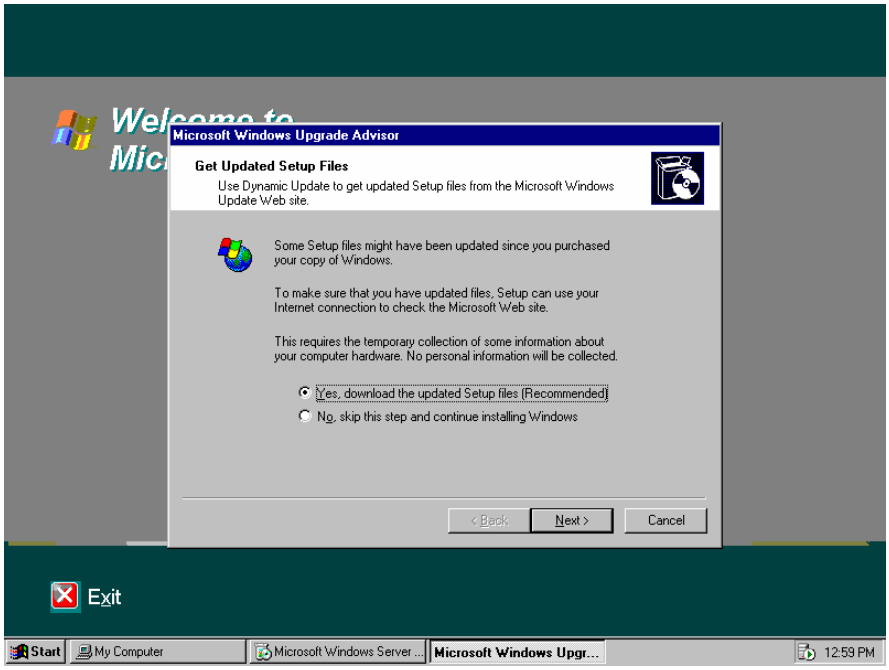

Microsoft Windows Upgrade Advisor
Get Updated Setup Files
Use Dynamic Update to get updated Setup files from the Microsoft Windows Update Web site.
Some Setup files might have been updated since you purchased your copy of Windows.
To make sure that you have updated files, Setup can use your Internet connection to check the Microsoft Web site.
This requires the temporary collection of some information about your computer hardware. No personal information will be collected.
Yes, download the updated Setup files (Recommended)
No, skip this step and continue installing Windows
< Back
Next >
Cancel
Exit
Start
My Computer
Microsoft Windows Server ...
Microsoft Windows Upgr...
12:59 PM

Figure 17. Option to get the most up to date setup files

After choosing the recommended procedure, Setup starts the upgrade process and prompts the user to accept the licensing agreement as shown in the following figure:

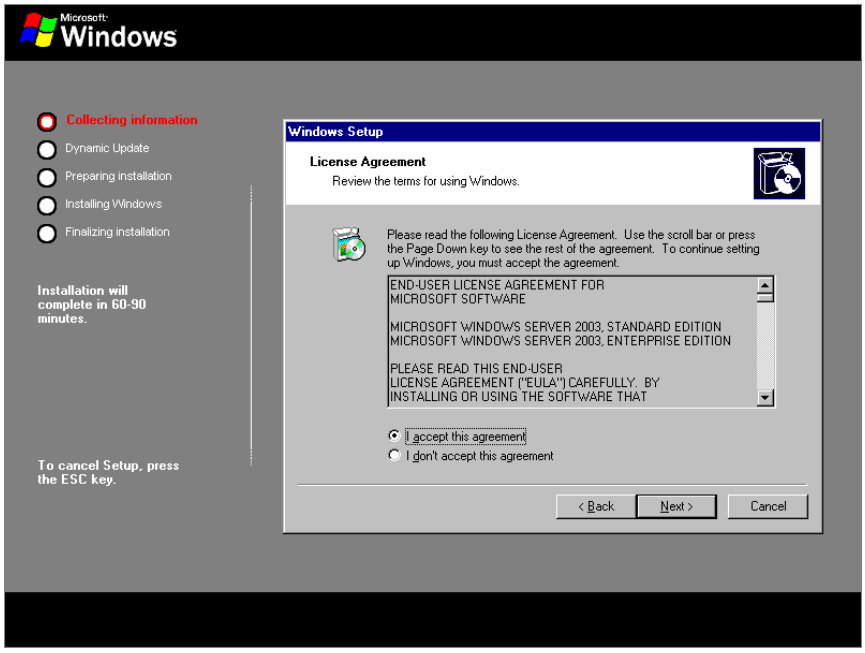

Microsoft Windows
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Installation will complete in 60-90 minutes.
To cancel Setup, press the ESC key.
Windows Setup
License Agreement
Review the terms for using Windows.
Please read the following License Agreement. Use the scroll bar or press the Page Down key to see the rest of the agreement. To continue setting up Windows, you must accept the agreement.
END-USER LICENSE AGREEMENT FOR MICROSOFT SOFTWARE
MICROSOFT WINDOWS SERVER 2003, STANDARD EDITION
MICROSOFT WINDOWS SERVER 2003, ENTERPRISE EDITION
PLEASE READ THIS END-USER LICENSE AGREEMENT ("EULA") CAREFULLY. BY INSTALLING OR USING THE SOFTWARE THAT
I accept this agreement
I don't accept this agreement
< Back
Next >
Cancel

Figure 18. Accepting the licensing agreement

After accepting the licensing agreement, the user must enter the Product Key as shown:

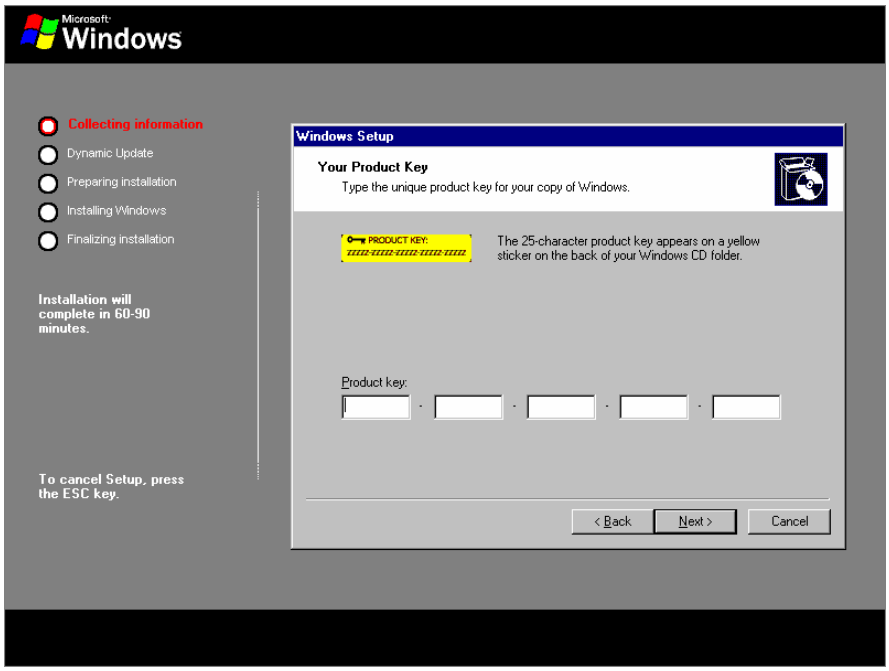


Figure 19. Product Key dialog box

Next, the user is prompted about the compatibility issues found earlier when running System Compatibility Checker. After the **Continue** button is selected, Setup is finished with the information collection tasks and continues to follow the roadmap found on the left panel of the setup screens. If necessary, Setup locates the latest setup files and starts the routine to prepare the installation. During this process, the sample server reboots itself and continues the process without user intervention. No more prompts for information appear until the upgrade is complete.

The upgrade finishes in one hour and fifteen minutes. The computer is set as a PDC, so after it reboots, Setup automatically launches the Active Directory Setup Wizard. For more information about upgrading to Active Directory, see Appendix A: Sample Active Directory Upgrade later in this guide.

Results of the Sample Windows NT Upgrade

Here are some notes worth mentioning:

- The Intel network adapter was automatically detected and worked as expected. The Kingston network card was not detected and did not work after the upgrade.
- Before the installation, the \Winnt folder was 262 MB. After the installation, it was 1.45 GB. This size increase is an important consideration, because drive C of most Windows NT servers is 4 GB or less. Disk space may be a deciding factor in whether to perform a new installation or perform an upgrade. Bear in mind that this example was not a production server; it had almost the maximum available disk space on the drive C partition. Production Windows NT servers that have been in service for some time typically do not have a large amount of free space on the boot partition.

- SQL Server 7.0 ran normally after upgrade, even though it is not officially supported on Windows Server 2003.
- All drivers, with the exception of the one network card, were automatically detected and worked as expected, including the SCSI adapter, Intel network adapter, and ATI video drivers.
- This sample upgrade did not test all possible services and was designed to show only a typical upgrade scenario with common applications and services. Other services such as WINS, DHCP, and Terminal Services, and so on were not tested.
- Exchange Server failed to start after the upgrade. If this were a production server, the mail server would no longer function. The Exchange System Attendant service and the Exchange Directory Service are the only Exchange services that restarted. All the Exchange services maintained their service account information, but most failed to start. When an attempt is made to start the Exchange Information Store, errors appear in Event Viewer as Figure 20 shows. To display detailed information, double-click an error.

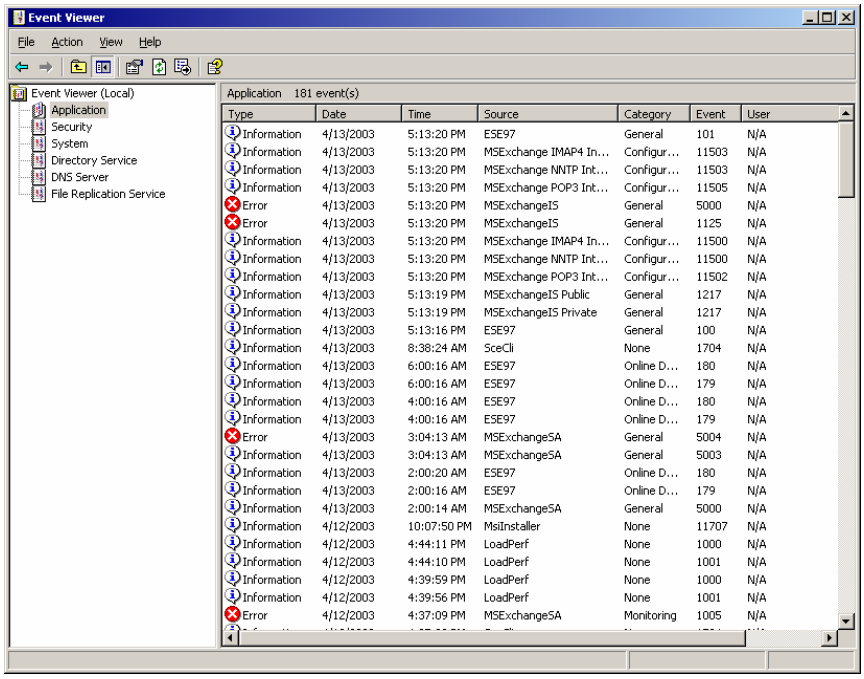

Event Viewer
File Action View Help
Event Viewer (Local)
Application
Security
System
Directory Service
DNS Server
File Replication Service
Application 181 event(s)
Type Date Time Source Category Event User
Information 4/13/2003 5:13:20 PM ESE97 General 101 N/A
Information 4/13/2003 5:13:20 PM MSExchange IMAP4 In... Configur... 11503 N/A
Information 4/13/2003 5:13:20 PM MSExchange NNTP Int... Configur... 11503 N/A
Information 4/13/2003 5:13:20 PM MSExchange POP3 Int... Configur... 11505 N/A
Error 4/13/2003 5:13:20 PM MSExchangeIS General 5000 N/A
Error 4/13/2003 5:13:20 PM MSExchangeIS General 1125 N/A
Information 4/13/2003 5:13:20 PM MSExchange IMAP4 In... Configur... 11500 N/A
Information 4/13/2003 5:13:20 PM MSExchange NNTP Int... Configur... 11500 N/A
Information 4/13/2003 5:13:20 PM MSExchange POP3 Int... Configur... 11502 N/A
Information 4/13/2003 5:13:19 PM MSExchangeIS Public General 1217 N/A
Information 4/13/2003 5:13:19 PM MSExchangeIS Private General 1217 N/A
Information 4/13/2003 5:13:16 PM ESE97 General 100 N/A
Information 4/13/2003 8:38:24 AM SceCli None 1704 N/A
Information 4/13/2003 6:00:16 AM ESE97 Online D... 180 N/A
Information 4/13/2003 6:00:16 AM ESE97 Online D... 179 N/A
Information 4/13/2003 4:00:16 AM ESE97 Online D... 180 N/A
Information 4/13/2003 4:00:16 AM ESE97 Online D... 179 N/A
Error 4/13/2003 3:04:13 AM MSExchangeSA General 5004 N/A
Information 4/13/2003 3:04:13 AM MSExchangeSA General 5003 N/A
Information 4/13/2003 2:00:20 AM ESE97 Online D... 180 N/A
Information 4/13/2003 2:00:16 AM ESE97 Online D... 179 N/A
Information 4/13/2003 2:00:14 AM MSExchangeSA General 5000 N/A
Information 4/12/2003 10:07:50 PM MsiInstaller None 11707 N/A
Information 4/12/2003 4:44:11 PM LoadPerf None 1000 N/A
Information 4/12/2003 4:44:10 PM LoadPerf None 1001 N/A
Information 4/12/2003 4:39:59 PM LoadPerf None 1000 N/A
Information 4/12/2003 4:39:56 PM LoadPerf None 1001 N/A
Error 4/12/2003 4:37:09 PM MSExchangeSA Monitoring 1005 N/A

Figure 20. Application log with Exchange IS errors

In this sample upgrade, the lesson is to pay particular attention to the system compatibility checker and research possible issues before the upgrade. For example, the detailed view of Event ID 5000 (one of the errors shown in Figure 20) looks like this:

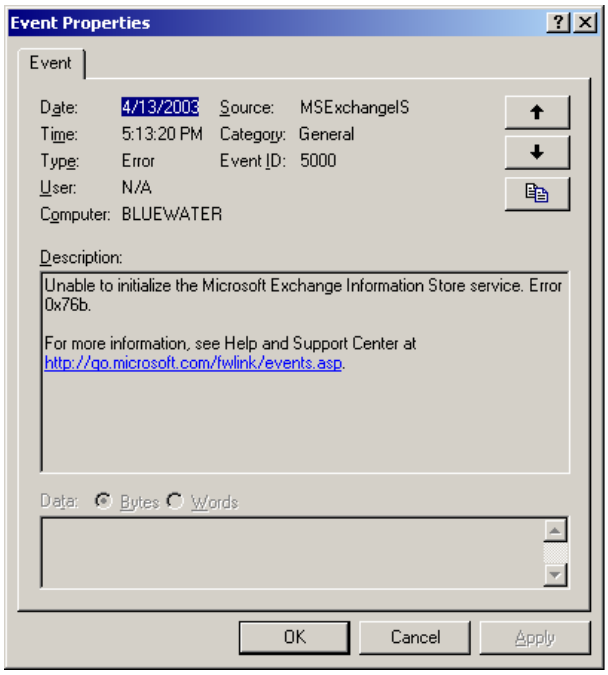


Figure 21. Detailed Exchange 5.5 Event ID

Sample Product Activation

After the server has been upgraded and problems are solved, it is time to think about product activation. This process is aimed at reducing software piracy as well as ensuring that Microsoft customers receive the product quality they expect.

Those who acquire software licenses through one of the Microsoft volume licensing programs are not required to activate those licenses. Microsoft understands the unique deployment requirements of businesses that need to acquire licenses in volume and provides products that do not require activation to those customers. Qualifying as a volume licensing customer is easier than many may think. Customers can qualify for Microsoft Open Licensing program by purchasing as few as five licenses. More information about Microsoft Open Licensing and other Microsoft volume licensing programs can be found on the Microsoft Licensing (http://www.microsoft.com/licensing/) Web site.

Software acquired as packaged product requires activation. Software acquired on new PCs sold by OEMs also requires activation; however, the software may be activated by the OEM at the factory before delivery to the end user.

Customers who activate their software must complete a simple, straightforward, and anonymous activation process that takes less than one minute when completed over the Internet. Activation can also be completed by telephoning Microsoft and speaking with a customer service representative. If activation is completed by using the Internet, the product takes care of most of the work and requires very little user participation. If activation is completed by telephoning Microsoft, a customer service representative assists with the activation.

Activation is not product registration. The only information required to activate a product is an installation ID created by the software and, for Office XP and Visio 2002, the country in which the software is being installed. No personally identifiable information is required to activate.

The software activation process works as follows:

1. A user is prompted to activate the product during setup or use.

Note The products have a grace period in which they can operate without being activated.

---

2. The user selects an activation method: Use the Internet or call Microsoft.
3. The Microsoft Activation Server processes the activation request and verifies that the software is legitimate.
4. If the user began the activation process over the Internet, the Microsoft Activation Server returns an activation confirmation silently to the client computer. If the request was handled over the telephone, the user receives the activation confirmation ID verbally, and then uses the ID to complete the activation.
5. The user software is activated.

Migrating to Active Directory

A directory stores information related to network resources and makes it possible to locate and manage these resources. A directory service is a network service that identifies all resources on a network and makes them accessible to users and applications. A directory service differs from a directory in that it is both the source of the information and the service making the information available to users.

Active Directory is the directory service included in Windows Server 2003. Active Directory includes the directory, which stores information related to network resources, and all the services that make this information available. Active Directory relies on DNS, so any Active Directory migration must carefully consider this service.

Benefits of Active Directory

Windows Server 2003 enhances administrators' abilities to efficiently configure and manage Active Directory in organizations of various sizes. Windows Server 2003 Active Directory service enables organizations to control the costs of managing their computer-based directories by using a single, unifying directory service. With Active Directory, employees can quickly locate information about network resources and administrators can easily manage the network from a central location. Ultimately, the efficiencies that Active Directory includes can reduce IT costs and help improve organizational productivity.

Windows Server 2003 makes it much easier to use Active Directory and includes new features, such as cross-forest trusts, the ability to rename domains, and the ability to deactivate attributes and classes in the schema so that their definitions can be changed. Organizations can also enjoy the following benefits:

- **Find information quickly.** At the simplest level, Active Directory is a database of information about users, computers, printers, and just about any computer-related item in the enterprise. Users benefit from Active Directory by being able to quickly find what they need—anywhere in the network. For example, Active Directory can serve much like a telephone directory by automatically locating the nearest printer, freeing users from having to know the correct name or address path of the printer.
- **Use improved management tools.** The improved upgrade and management tools along with the ability to rename Active Directory domains make deploying Active Directory significantly easier than when the directory service was first introduced in Windows 2000 Server.

Upgrading and planning are more efficient with the following features:

- **Active Directory Migration Tool (ADMT) 2.0.** It is now easier to upgrade to Active Directory through a number of improvements that have been made to ADMT 2.0. The tool now allows passwords to be upgraded from Windows NT 4.0 to Windows 2000 and Windows Server 2003 domains or from Windows 2000 to Windows Server 2003 domains.
- **Domain renaming.** Administrators can now change the DNS or NetBIOS names of existing domains in a forest while keeping the resulting forest well formed. Administrators also have

greater flexibility in changing the Active Directory structure after it is deployed. Design decisions are now reversible, which benefits organizations that merge or restructure departments.

- **Schema redefinition.** The flexibility of Active Directory has been enhanced to allow the deactivation of attributes and class definitions in the Active Directory schema. Attributes and classes can be redefined if an error was made in the original definition.

Improved Management with Group Policy

Organizations still using Windows NT 4.0 can significantly lower costs by taking advantage of the efficiencies enabled by Group Policy and Active Directory. Although Windows NT 4.0 provided rudimentary tools to set policies, they were set on a server-by-server basis and hard to administer. With Group Policy in Windows Server 2003, policies can be set for desktop and servers and then automatically applied to as many desktops and servers as necessary with Active Directory. As Figure 22 shows, through Active Directory and Group Policy, administrators can apply policy-based management to enable one-to-many management of users and computers throughout the enterprise and automate enforcement of IT policies.

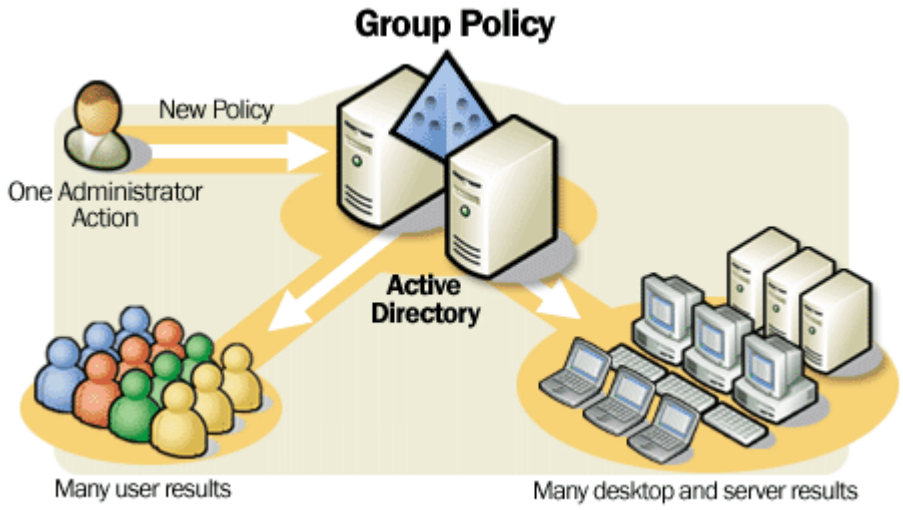


Figure 22. Group Policy enables one-to-many management of users and computers throughout an organization

Group Policy in Windows Server 2003 provides benefits in the following areas:

- **Enhanced security.** Administrators can easily define and automatically enforce software security policies.
- **Improved customer satisfaction and reduced Help Desk costs.** Administrators can enforce standardized desktop and server environments. This capability decreases the risk of broken software configurations and user error, while improving an IT organization's ability to troubleshoot problems.
- **Increased data safety and availability.** Administrators can provide automated folder redirection, data backup, and data recovery by using Group Policy.

- **Flexible control over the computing environment.** Administrators can define and enforce organizational standards through Group Policy and can rapidly reconfigure Group Policy settings to adapt to changing business requirements. Group Policy implementations also scale from small work group environments to high-end data centers and can be used to simulate and validate the impact of any changes before applying them to production environments.
- **Increased productivity.** Administrators can manage an entire group of users and IT assets as easily as managing a single entity. Group Policy helps administrators respond rapidly to required changes in group configurations or policy enforcements, a benefit that helps organizations run their IT operations more effectively. Scripting of Group Policy operations can provide even greater IT workload efficiencies

Windows NT Server 4.0 Upgrade Design and Planning

The Windows Server 2003 Active Directory service is compatible with Windows NT Server 4.0 and includes a mix of operations through which domain controllers running Windows NT Server 4.0, Windows 2000, and Windows Server 2003 can be supported. As a result, organizations can upgrade domains and computers at an established pace based on the organization's needs.

Active Directory supports the Windows NT LAN Manager (NTLM) protocol used by Windows NT. This support enables authorized users and computers from a Windows NT domain to log on and access resources in Windows 2000 or Windows Server 2003 domains. To clients running Windows 95, Windows 98, or Windows NT that are not running Active Directory client software, a Windows 2000 or Windows Server 2003 domain appears to be a Windows NT Server 4.0 domain. For more information, see “Active Directory Clients” in the Windows Server 2003 on-screen Help and Support Center.

Preparing for Active Directory

Preparing a Windows NT 4.0 domain for Active Directory requires a considerable amount of planning and education. Windows NT 4.0 administrators must understand the differences between Windows NT domains and Windows Server 2003 domains. One of the most common mistakes is to plan the Active Directory domain as if it were a Windows NT domain. In many cases, the number of domains in an Active Directory domain structure can be reduced through the use of organizational units.

It takes time to understand the changes that occur when upgrading to Active Directory. One of the biggest changes is the dependency on DNS. It cannot be emphasized enough how important DNS is to the health of Active Directory and all the services that make up Active Directory. DNS implementation must be carefully planned so that it runs properly; otherwise, chances are there will be problems with the Active Directory services. For more information, the following documents are recommended:

- DNS and Microsoft Windows NT 4.0 Paper
- Windows 2000 DNS White Paper (2003 version not available yet)
- *DNS and BIND* by Paul Albitz and Cricket Liu (O’Reilly and Associates)

The two guides provide a great starter kit into the world of DNS for Windows NT administrators.

Another major area of study especially important to Windows NT administrators are the Flexible Single Master Operations Roles (FSMO) roles. The PDC emulator role can be crucial to the success of an upgrade to Windows Server 2003 Active Directory from Windows NT 4.0. This role emulates the functions of a PDC for pre-Windows 2000 clients.

What follows are guidelines for devising a high-level Active Directory infrastructure design.

Design a Forest Plan

One of the first decisions in Active Directory planning is how many forests are present in an organization. A forest is essentially a boundary for a domain or multiple domains. All domains in a forest share a common Active Directory schema. The Active Directory schema defines the objects that can be stored in Active Directory. An object is a distinct named set of attributes that represents a network resource. Object attributes are characteristics of objects in the directory. For example, a printer object has a *name*, *location*, *driver*, and so on. These attributes make up a printer object and define how the object works. The goal of any upgrade is to minimize the number of forests, and thus the number of schemas. The ultimate goal is to have only one forest, but this ideal is not always practical. For example, maybe an organization has two distinct businesses that do not interact with one another. They are independent, even though they live under the same corporate umbrella. In such a case, two forests are necessary.

Making changes to the schema can have enterprise-wide ramifications, so a schema modification policy is important at this stage. This policy defines who can make changes to the schema. These changes propagate to all domains and domain controllers in the forest, so it is an important policy.

Design a Domain Plan

When designing the domain plan, keep in mind that Active Directory may enable you to use fewer domains than Windows NT 4.0. OUs did not exist in Windows NT 4.0 domains. An OU is a container used to organize objects within a domain into a logical administrative group.

With Windows NT 4.0 domains, if an enterprise administrator wanted to allow an administrator in a remote location to administer their own network resources without administering all network resources in the enterprise, it required another domain to be installed. OUs perform the same function in Active Directory. Using an OU, an enterprise administrator can grant administrative access to a local administrator for all objects located at the remote location but prohibit access to objects outside that OU.

The domain design phase should also evaluate the number of domains to be upgraded and why those domains were created in the first place. If a domain can be retired and replaced by an OU, the upgrade plans should include the removal of unnecessary domains—a scenario known as domain consolidation.

Designing an OU Plan

When determining the OUs to include, it is important to understand an OU's purpose. Fundamentally, an OU serves three purposes:

- Provides logical groupings of objects (for locating objects).

- Helps in the application of Group Policy.
- Provides administrative groupings of objects (for administrative purposes).

Keeping these purposes in mind, you can now define the OUs, users, and groups based on the structure of your organization. It is worth mentioning that there is a big difference between OUs and groups. As mentioned, OUs are used to organize objects for administrative purposes, such as delegation. However, OUs cannot be used to apply permissions or rights. Groups are used to apply permissions and rights. OUs can be defined based on a number of items, including organizational function or physical location.

The end result of an OU plan depicts the following:

- A diagram of OU structures for each domain.
- A list of users in each OU.
- A list of groups in each domain.

Designing a Site Topology Plan

Sites are typically used to represent physical locations separated by slow wide area network (WAN) links. Creating a site topology includes performing the following tasks:

- Defining sites
- Placing domain controllers
- Defining a replication strategy
- Configuring bridgehead servers
- Placing global catalog servers
- Placing operations masters

A site topology plan should include a site diagram with placement of domain controllers, locations of operations masters, types of site links, and documentation regarding the types of site links and their corresponding configurations.

Connectivity with Windows NT Server 4.0, Windows 2000, and Windows Server 2003

Domain and forest functionality, introduced in Windows Server 2003 Active Directory, are extensions of mixed and native modes for Windows 2000-based networks. They provide a way to enable domain-wide or forest-wide Active Directory features in a network environment.

You can raise the functional level of a domain to enable new Active Directory features that apply to that domain only. There are four domain functional levels:

- Windows 2000 mixed
- Windows 2000 native
- Windows Server 2003 interim
- Windows Server 2003

The default domain functional level is Windows 2000 mixed. Additional Active Directory features become available when the domain functional level is raised to Windows 2000 native, Windows Server 2003 interim, or Windows Server 2003. Use the Active Directory Users and Computers snap-in to adjust or determine the domain functional level as Figures 23 and 24 show.

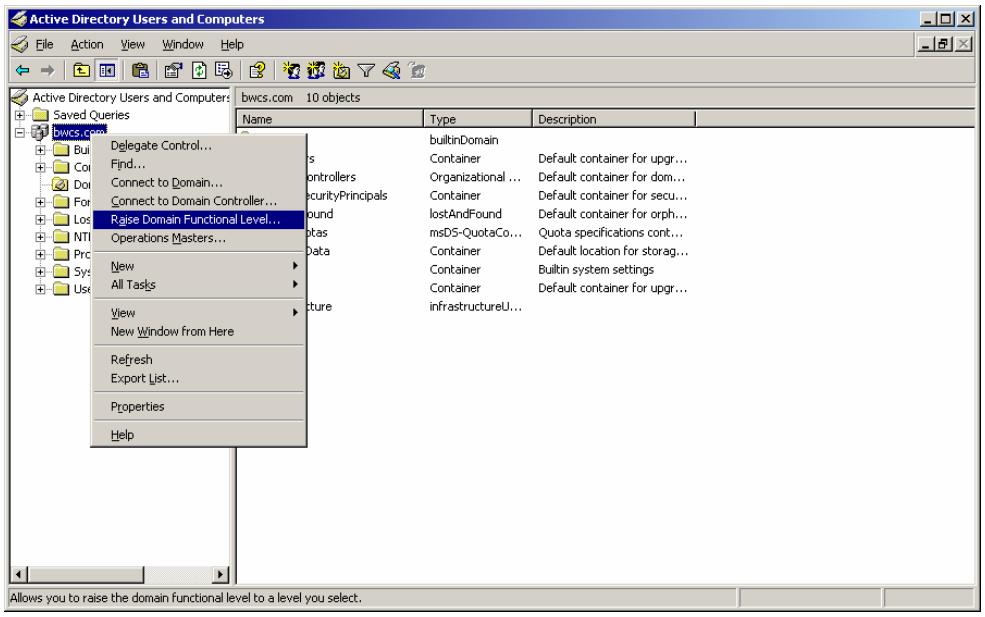


Figure 23. Setting the domain functional level

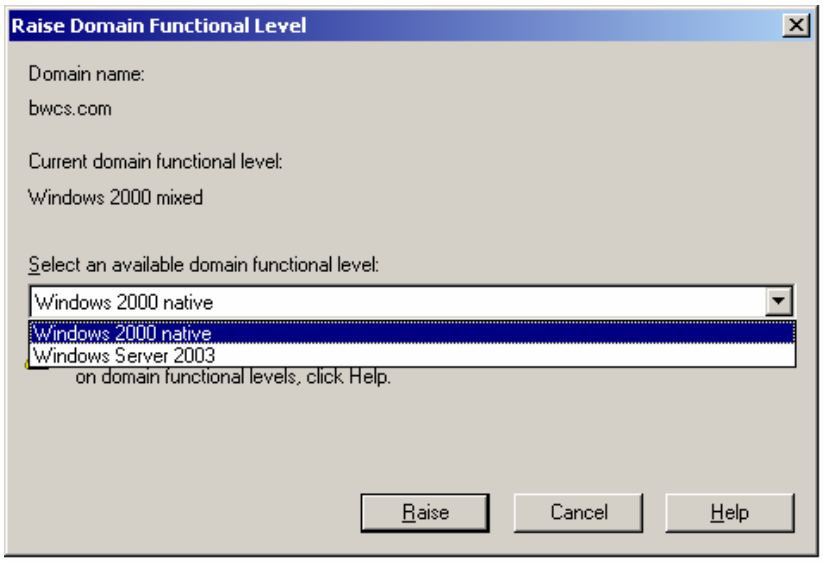


Figure 24. Detailed view of changing the domain functional level

Forest functionality enables features across all the domains in a forest. There are three forest functional levels:

- Windows 2000

- Windows Server 2003 interim
- Windows Server 2003

When you upgrade a Windows NT 4.0 PDC to Windows Server 2003, the *Windows Server 2003 interim functional* level is initialized automatically. The Windows Server 2003 interim functional level supports both Windows NT 4.0 domain controllers and Windows Server 2003 domain controllers. The Windows Server 2003 interim functional level is ideal if you have groups that include over 5,000 members in the existing Windows NT 4.0 environment. It's best to remain at this functional level until after you upgrade all of the other Windows NT 4.0 domain controllers to Windows Server 2003.

Note If the forest functional level is set to Windows 2000, the level cannot be changed to Windows Server 2003 interim through the Active Directory administrative consoles.

The Active Directory administrative consoles cannot be used to change the forest functional level from Windows 2000 to Windows Server 2003 interim. Although this limitation should not be an issue when performing an in-place domain upgrade, it may be an issue if migrating to a new side-by-side Windows Server 2003 domain.

To raise the forest or domain functional level to Windows Server 2003 interim, you must use a Lightweight Directory Access Protocol (LDAP) application, such as ADSI Edit or Ldp (found in the Windows Support Tools) to edit the value of the *msDS-Behavior-Version* attribute. You must be logged on as a member of the Enterprise Admins group to modify this attribute. You can use the Active Directory Domains and Trusts snap-in to change the forest functional level as Figures 25 and 26 show.

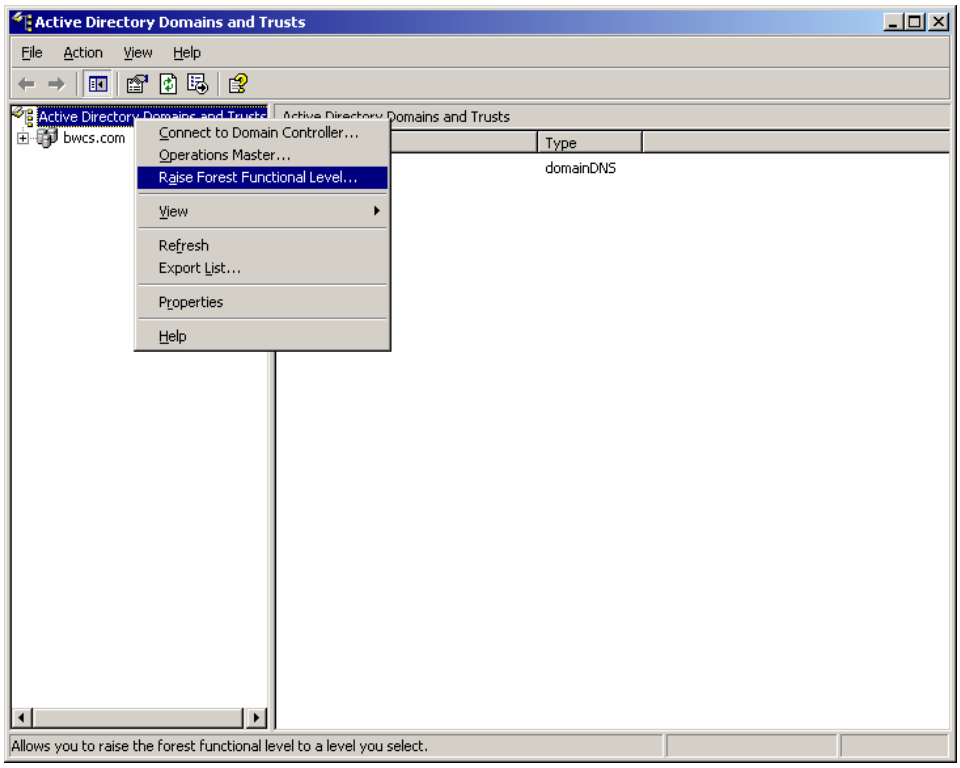


Figure 25. Setting the forest functional level

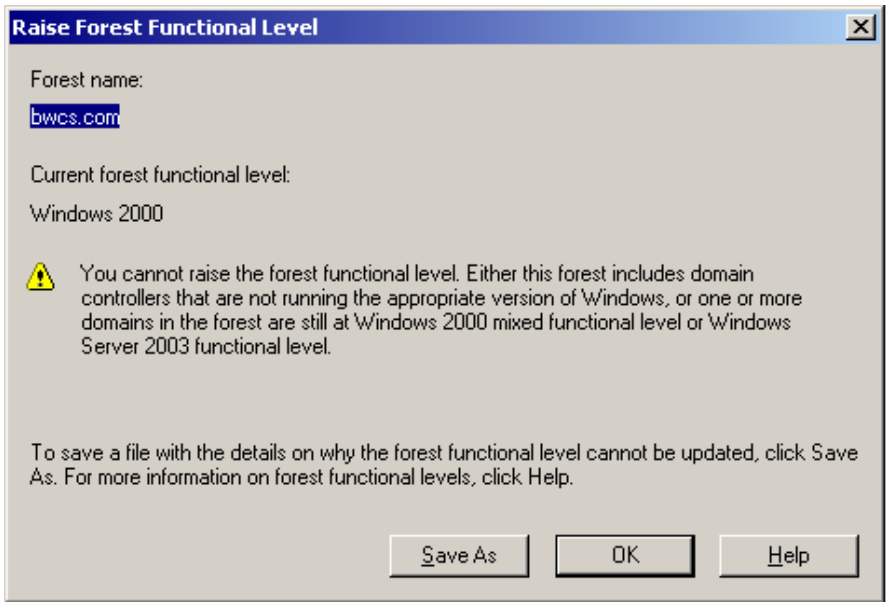

Raise Forest Functional Level
Forest name:
bwcs.com
Current forest functional level:
Windows 2000
You cannot raise the forest functional level. Either this forest includes domain controllers that are not running the appropriate version of Windows, or one or more domains in the forest are still at Windows 2000 mixed functional level or Windows Server 2003 functional level.
To save a file with the details on why the forest functional level cannot be updated, click Save As. For more information on forest functional levels, click Help.
Save As
OK
Help

Figure 26. Error trying to raise the forest functional level

For more information about enabling functional levels in a Windows NT 4.0 environment, see Enabling Functional Levels on the TechNet Web site.

Upgrading a Windows NT Domain to Active Directory

After the high-level planning phase, it is time to start implementing the plan. The upgrade process involves the following steps:

- Plan and implement a namespace and DNS infrastructure.
- Determine forest functionality.
- Upgrade the server running Windows NT Server 4.0 or earlier PDC.
- Upgrade any remaining BDCs.
- Convert groups.
- Complete the upgrade of the domain.

Planning and Implementing a Namespace and DNS Infrastructure

Namespace refers to the naming convention that defines a set of unique names for resources in a network, such as DNS, a hierarchical naming structure that identifies each network resource and its place in the hierarchy of the namespace, and WINS, a flat naming structure that identifies each network resource using a single, unique name.

DNS is required for Active Directory. DNS is a hierarchical, distributed database that contains mappings of DNS domain names to various types of data, such as IP addresses. DNS enables the location of computers and services by user-friendly names, and it also enables the discovery of other information stored in the database.

When setting up a namespace, it is recommended that you first choose and register a unique parent DNS domain name that can be used for hosting your organization on the Internet, for example, Microsoft.com. Once you have chosen your parent domain name, you can combine this name with a location or organizational name used in your organization to form other subdomain names. For example, a subdomain can be added for resources used by the information technology group at your organization, called itg.example.microsoft.com domain tree. Additional subdomain names can then be formed using this name, such as edi.itg.example.microsoft.com, a subdomain for a group of programmers working on electronic data interchange (EDI) in this division. Likewise, another group of workers providing support in this division might use support.itg.example.microsoft.com.

Before beginning the upgrade from Windows NT Server 4.0 to the Windows Server 2003 Active Directory service, ensure that you have designed a DNS and Active Directory namespace and have either configured DNS servers or are planning to have the Active Directory Installation Wizard automatically install the DNS service on the domain controller.

Active Directory and DNS Integration

Active Directory is integrated with DNS in the following ways:

- Active Directory and DNS have the same hierarchical structure. Although separate and implemented differently for different purposes, an organization's namespace for DNS and Active Directory have an identical structure. For example, microsoft.com is both a DNS domain and an Active Directory domain.

- DNS zones can be stored in Active Directory. If you are using the Windows Server DNS service, primary zone files can be stored in Active Directory for replication to other Active Directory domain controllers.
- Active Directory uses DNS as a locator service, resolving Active Directory domain, site, and service names to an IP address. To log on to an Active Directory domain, an Active Directory client queries its configured DNS server for the IP address of the LDAP service running on a domain controller for a specified domain. For more information on how Active Directory clients rely on DNS, see "Locating a Domain Controller" in the Windows Server 2003 on-screen Help and Support Center.

Active Directory and DNS Differences

While Active Directory is integrated with DNS and they share the same namespace structure, it is important to distinguish the basic difference between them:

- **DNS is a name resolution service.** DNS clients send DNS name queries to their configured DNS server. The DNS server receives the name query and either resolves the name query through locally stored files or consults another DNS server for resolution. DNS does not require Active Directory to function.
- **Active Directory is a directory service.** Active Directory provides an information repository and services to make information available to users and applications. Active Directory clients send queries to Active Directory servers using LDAP. To locate an Active Directory server, an Active Directory client queries DNS. Active Directory requires DNS to function.

For more information on DNS configuration, see the Windows Server 2003 on-screen Help and Support Center.

Flexible Single Master Operations Roles (FSMO)

In a forest, at least five FSMO roles are assigned to one or more domain controllers. The five FSMO roles are:

- **Schema master.** The schema master domain controller controls all updates and modifications to the schema. To update the schema of a forest, you must have access to the schema master. There can be only one schema master in the whole forest.
- **Domain naming master.** The domain naming master domain controller controls the addition or removal of domains in the forest. There can be only one domain naming master in the whole forest.
- **Infrastructure master.** The infrastructure is responsible for updating references from objects in its domain to objects in other domains. At any one time, there can be only one domain controller acting as the infrastructure master in each domain.
- **Relative ID (RID) master.** The RID master is responsible for processing RID pool requests from all domain controllers in a particular domain. At any one time, there can be only one domain controller acting as the RID master in the forest.

- **PDC emulator.** The PDC emulator is a domain controller that advertises itself as the PDC to workstations, member servers, and domain controllers that are running earlier versions of Windows. For example, if the domain contains computers that are not running Microsoft Windows XP Professional or Microsoft Windows 2000 client software, or if it contains Microsoft Windows NT BDCs, the PDC emulator master acts as a Windows NT PDC. It is also the domain master browser, and it handles password discrepancies. At any one time, there can be only one domain controller acting as the PDC emulator master in each domain in the forest.

You can transfer FSMO roles by using a Microsoft Management Console (MMC) snap-in tool. Depending on the FSMO role that you want to transfer, you can use one of the following three MMC snap-in tools:

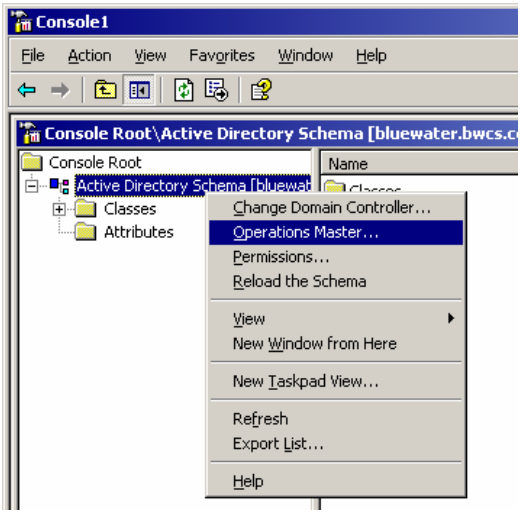
- Active Directory Schema snap-in
- Active Directory Domains and Trusts snap-in
- Active Directory Users and Computers snap-in

If a computer no longer exists, its role must be seized. However, if the server providing an FSMO role is down, its FSMO roles do not need to be seized necessarily—particularly if the server will be fixed and brought back online. Care must be taken to ensure a role is not seized if the original server holding the role will be returned to service. Allowing a situation where multiple servers are attempting to provide the same FSMO role can cause problems in Active Directory. Provided it is necessary to seize a role, use the following procedures to seize a role using one of the MMC snap-ins from the bulleted list.

To transfer the schema master role, do the following:

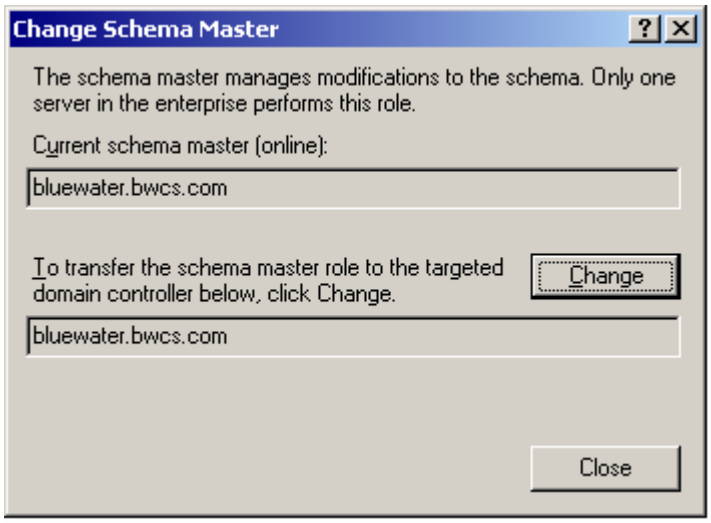
1. Click **Start**, click **Run**, type **mmc** in the **Open** box, and then click **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**.
3. Click **Add.**
4. Click **Active Directory Schema**, click **Add**, click **Close**, and then click **OK**.
5. In the console tree, right-click **Active Directory Schema**, and then click **Change Domain Controller**.
6. Click **Specify Name**, type the name of the domain controller that will be the new role holder, and then click **OK**.
7. Right-click **Active Directory Schema**, and then click **Operation Masters**.
8. Click **Specify Name**, type the name of the domain controller that you want to hold the schema master role, and then click **OK**.

9. In the console tree, right-click **Active Directory Schema**, and then click **Operations Master.**



10. Click **Change**.

11. Click **OK** to confirm that you want to transfer the role, and then click **Close**.


Change Schema Master
The schema master manages modifications to the schema. Only one server in the enterprise performs this role.
Current schema master (online):
bluewater.bwcs.com
To transfer the schema master role to the targeted domain controller below, click Change.
Change
bluewater.bwcs.com
Close

To transfer the domain naming master role, do the following:

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Domains and Trusts**.
2. Right-click **Active Directory Domains and Trusts**, and then click **Connect to Domain Controller**.

Note You must perform this step if you are not on the domain controller to which you want to transfer the role. You do not have to perform this step if you are already connected to the domain controller whose role you want to transfer.

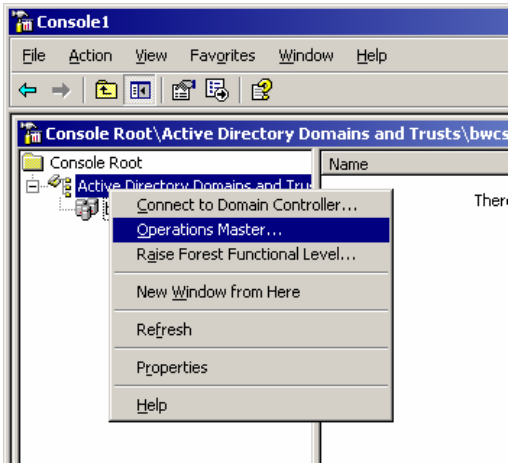
---

3. Do one of the following:

   - In the **Enter the name of another domain controller** box, type the name of the domain controller that will be the new role holder, and then click **OK**.

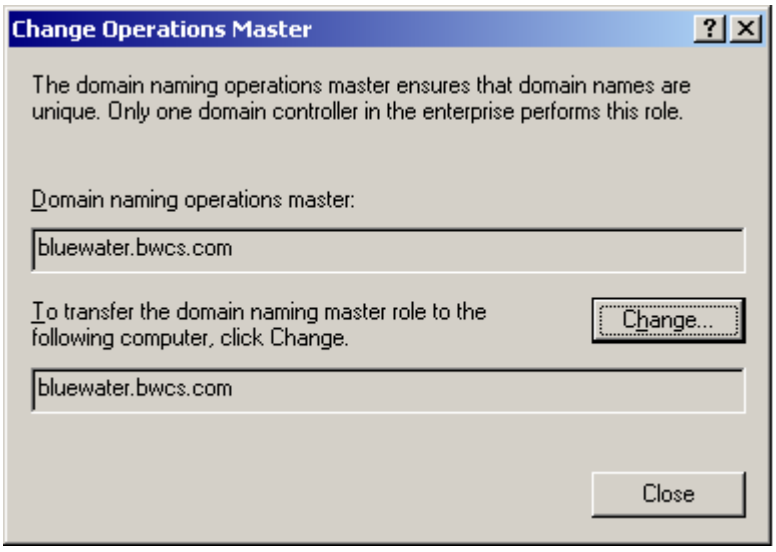
   —OR—

   1. In the **or, select an available domain controller** list, click the domain controller that will be the new role holder, and then click **OK**.
   2. In the console tree, right-click **Active Directory Domains and Trusts**, and then click **Operations Master**.



   3. Click **Change**.

4. Click **OK** to confirm that you want to transfer the role, and then click **Close**.


Change Operations Master
The domain naming operations master ensures that domain names are unique. Only one domain controller in the enterprise performs this role.
Domain naming operations master:
bluewater.bwcs.com
To transfer the domain naming master role to the following computer, click Change.
Change...
bluewater.bwcs.com
Close

To transfer the RID master, PDC emulator, and infrastructure master roles, do the following:

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. Right-click **Active Directory Users and Computers**, and then click **Connect to Domain Controller**.

Note You must perform this step if you are not on the domain controller to which you want to transfer the role. You do not have to perform this step if you are already connected to the domain controller whose role you want to transfer.

---

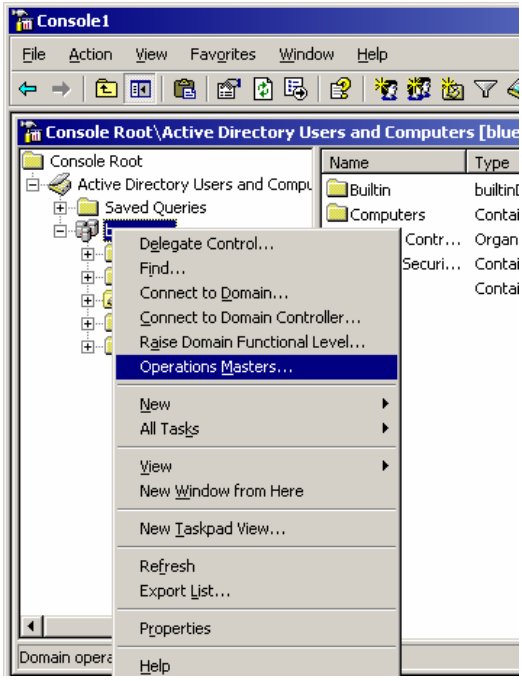
3. Do one of the following:

   - In the **Enter the name of another domain controller** box, type the name of the domain controller that will be the new role holder, and then click **OK**.

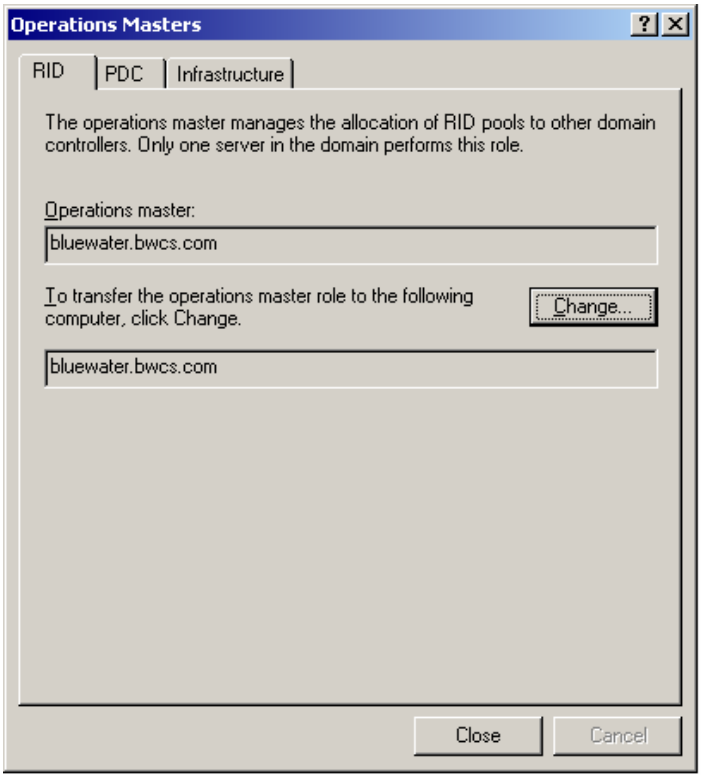
   —OR—

   1. In the **or, select an available domain controller** list, click the domain controller that will be the new role holder, and then click **OK**.

2. In the console tree, right-click **Active Directory Users and Computers**, point to **All Tasks**, and then click **Operations Master**.



3. Click the appropriate tab for the role that you want to transfer (**RID**, **PDC**, or **Infrastructure**), and then click **Change**.



4. Click **OK** to confirm that you want to transfer the role, and then click **Close**.

Determining Forest Functionality

Forest functionality determines the type of Active Directory features that can be enabled in the scope of a single forest. Each forest functional level has a set of specific minimum requirements for the version of operating system that domain controllers throughout the forest can run. For example, the Windows forest functional level requires that all domain controllers run Windows Server 2003 operating systems.

In the scenario where you are upgrading your first Windows NT domain so that it becomes the first domain in a new Windows Server 2003 forest, it is recommended that you set the forest functional level to Windows interim. (You are prompted during the upgrade.) This level contains all the features used in the Windows 2000 forest functional level and also includes two important advanced Active Directory features:

- Improved replication algorithms made to the intersite topology generator.
- Replication improvements made to group memberships.

The Windows interim functional level is an option when upgrading the first Windows NT domain to a new forest and can be manually configured after the upgrade. For more information about how to set this functional level manually, see Windows Deployment and Resource Kits on the Windows Web site. The Windows interim forest functional level supports only domain controllers running Windows and Windows NT, not domain controllers running Windows 2000. Servers running Windows 2000 cannot be promoted to a domain controller in a forest where the forest functional level has been set to Windows interim.

Upgrading the Windows NT Server 4.0 or Earlier PDC

The first server running Windows NT Server 4.0 that you must upgrade is the PDC. Upgrading the Windows NT PDC is required for a successful upgrade of the domain. During the upgrade, the Active Directory Installation Wizard requires that you choose to join an existing domain tree or forest or start a new domain tree or forest. If you decide to join an existing domain tree, you must provide a reference to the appropriate parent domain. For more information, see “Checklist: Installing a Domain Controller” in the Windows Server 2003 on-screen Help and Support Center.

Running the Active Directory Installation Wizard installs all necessary components on the domain controller, such as the directory data store, and the Kerberos v5 protocol authentication software. After Kerberos has been installed, the setup process starts the authentication service and the ticket granting service. In addition, if the domain controller represents a new child domain, a transitive trust relationship is established with the parent domain. Eventually, the domain controller from the parent domain copies all schema and configuration information to the new child domain controller. The existing SAM objects are copied from the registry to the new data store. These objects are security principals.

During the upgrade, objects are created to contain the accounts and groups from the Windows NT domain. These Container objects—named Users, Computers, and Built-in—appear as folders in Active Directory Users and Computers. User accounts and predefined groups are placed in the Users folder. Computer accounts are placed in the Computers folder. Built-in groups

are placed in the Built-in folder. Note that these special Container objects are not organizational units. They cannot be moved, renamed, or deleted.

Existing Windows NT Server 4.0 and earlier groups are located in different folders depending on the nature of the group. Windows NT Server 4.0 and earlier built-in local groups (such as Administrators and Server Operators) are located in the Built-in folder. Windows NT Server 4.0 and earlier global groups (such as Domain Admins) and any user-created local and global groups are located in the Users folder.

The upgraded PDC can synchronize security principal changes among the remaining Windows NT Server 4.0 and earlier BDCs. It is recognized as the domain master by servers running Windows NT Server 4.0 and earlier BDCs.

If a domain controller running Windows Server 2003 goes offline or otherwise becomes unavailable, and no other Windows Server 2003 domain controllers exist in the domain, a Windows NT BDC can be promoted to a PDC to fill the role for the offline Windows Server 2003 domain controller.

The upgraded domain controller is a fully functional member of the forest. The new domain is added to the domain and site structure, and all domain controllers receive the notification that a new domain has joined the forest.

Upgrading Any Remaining BDCs

After you have upgraded the Windows NT Server 4.0 and earlier PDC, you can continue to upgrade all remaining BDCs. During the upgrade process, you may want to remove one BDC from the network as a precaution in case a problem develops. This BDC stores a copy of your current domain database.

If any problems arise during the upgrade, you can remove all domain controllers running Windows from the production environment, and then bring the BDC back into your network and make it the new PDC. This new PDC then replicates its data throughout the domain so that the domain is returned to its previous state.

The only drawback to this method is that all changes that were made while the isolated BDC was offline are lost. To minimize this loss, you can periodically turn the offline BDC on and off—when the domain is in a stable state—during the upgrade process to update its copy of the directory.

When upgrading Windows NT Server 4.0 and earlier domains, only one domain controller running Windows Server 2003 can create security principals (users, groups, and computer accounts). This single domain controller is configured as a PDC emulator master. The PDC emulator master emulates a Windows NT Server 4.0 and earlier PDC. For more information about the PDC emulator role, see “Operations Master Roles” in the Windows Server 2003 on-screen Help and Support Center.

Converting Groups

When you upgrade a PDC running Windows NT Server 4.0 to a server running Windows Server 2003, existing Windows NT groups are converted. Specifically, when the Windows Server 2003

domain is switched to native mode, Windows NT local groups are converted to domain local groups on servers running Windows Server 2003.

Domain member computers running Windows NT can continue to display and access the converted groups. The groups appear to these clients as Windows NT Server 4.0 local and global groups. However, a Windows NT client cannot display members of groups or modify the member properties when that membership violates Windows NT group rules. For example, when a Windows NT client views the members of a global group on a server running Windows Server 2003, it does not view any other groups that are members of that global group.

Using Converted Groups with Servers Running Windows Server 2003

Client computers that do not run Active Directory client software identify groups with universal scope on servers running Windows Server 2003 as having global scope instead. When viewing the members of a group with universal scope, the Windows NT client can only view and access group members that conform to the membership rules of global groups on servers running Windows Server 2003.

In a Windows Server 2003 domain that is set to a domain functional level of Windows 2000 native, all the domain controllers must run on servers that run Windows Server 2003. However, the domain can contain member servers that run Windows NT Server 4.0. These servers view groups with universal scope as having global scope and can assign groups with universal scope rights and permissions and place them in local groups.

In a Windows Server 2003 domain, a Windows NT Server 4.0 member server running Windows NT administrative tools cannot access domain local groups. However, you can work around this by using a server running Windows Server 2003 and using the administrative tools in its Windows Server 2003 Administration Tools Pack to access the server running Windows NT Server 4.0. You can use these tools to display the domain local groups and assign to them permissions to resources on the server running Windows NT Server 4.0.

Completing the Upgrade of the Domain

If you have upgraded all existing Windows NT Server 4.0 and earlier PDCs and BDCs to Windows Server 2003, and you have no plans to use Windows NT Server 4.0 and earlier domain controllers, you can raise the domain functional level from Windows 2000 mixed to Windows 2000 native.

Several things happen when you raise the domain functional level to Windows 2000 native:

- Domain controllers no longer support NTLM replication.
- The domain controller that is emulating the PDC operations master cannot synchronize data with a Windows NT Server 4.0 and earlier BDC.
- Windows NT Server 4.0 and earlier domain controllers cannot be added to the domain. (You can add new domain controllers running Windows 2000 or Windows Server 2003.)
- Users and computers using previous versions of Windows begin to benefit from the transitive trusts of Active Directory and (with the proper authorization) can access resources anywhere in the forest. Although previous versions of Windows do not support the Kerberos v5 protocol, the

pass-through authentication provided by the domain controllers allows users and computers to be authenticated in any domain in the forest. This authentication enables users or computers to access resources in any domain in the forest for which they have the appropriate permissions.

Other than the enhanced access to any other domains in the forest, clients are not aware of any changes in the domain.

Sample Active Directory Migration Plan

There are many ways to upgrade a Windows NT 4.0 domain to a Windows Server 2003 Active Directory domain. In the sample upgrade scenario that follows, one such way is documented. The sample upgrade scenario has been kept rather simple to fit in the context of this guide. It does, however, serve as a roadmap for many typical Windows NT 4.0 upgrades. Planning is the key component. A solid plan helps an upgrade team with even the most complicated Windows NT upgrade scenario.

In this sample, HGF Properties is a fictitious Southern California-based company with four locations. The company would like to upgrade from their current Windows NT 4.0 structure to Windows Server 2003 and Active Directory. This section walks through some of the steps involved in the upgrade of a small, single-domain network.

Figure 27 shows the current sites, domain, and servers for HGF Properties.

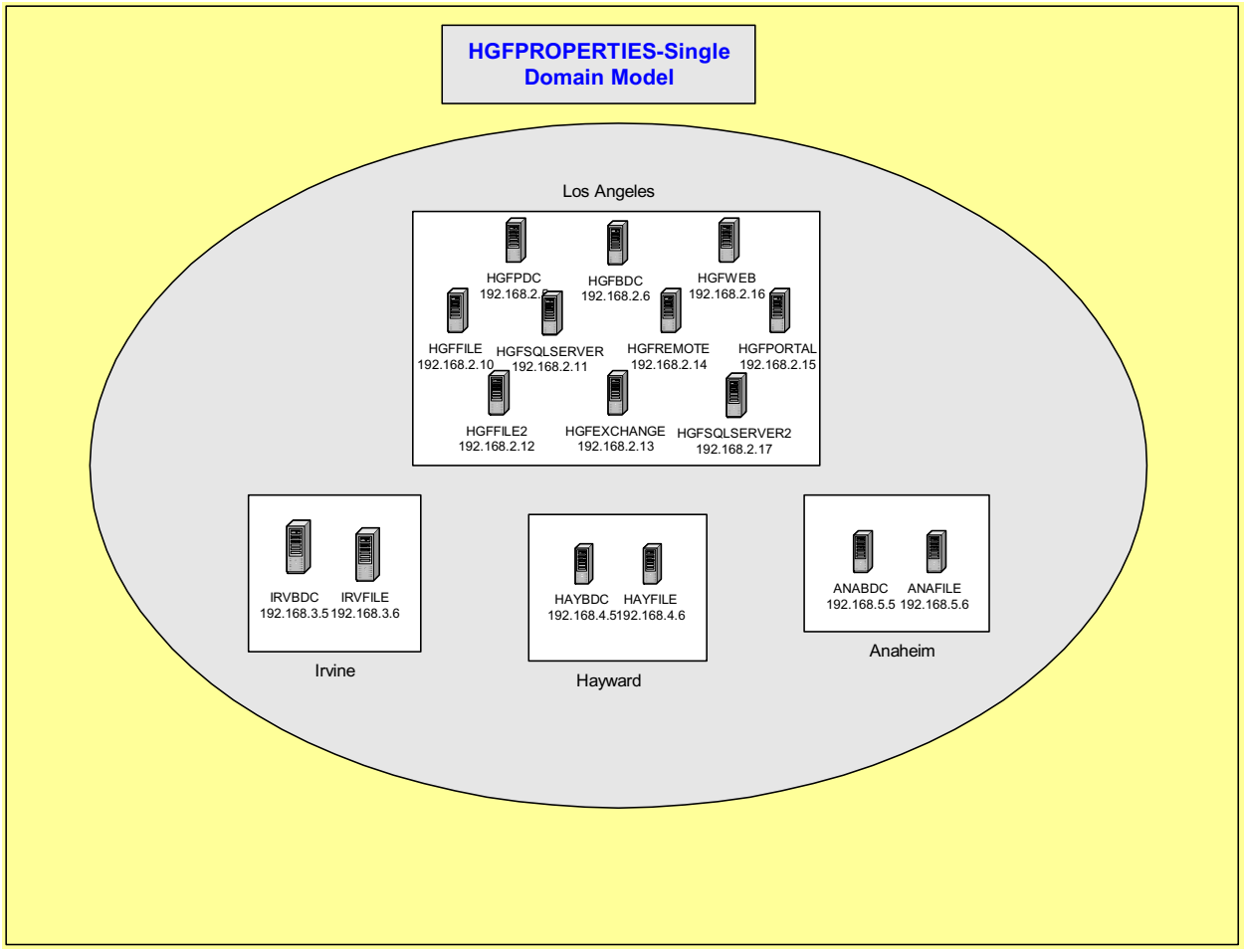


Figure 27. HGF Properties Windows NT 4.0 Single Domain Model

Server List

HGF Properties has a single domain called HGFPROPERTIES spread across four different locations. The table below lists the servers and their corresponding roles.

Servers for HGF Properties and the Roles They Perform

Server Name	Role	Version
HGFPDC	PDC for the entire organization	Windows NT 4.0 SP6
HGFBDC	BDC for Los Angeles location; running DHCP and WINS services	Windows NT 4.0 SP6
HGFFILE	File and print services and Accounting server	Windows NT 4.0 SP6
HGFSQLSERVER	SQL Server 6.5 database for internal custom application	Windows NT 4.0 SP6
HGFREMOTE	Remote access server running Terminal Services	Windows 2000 SP3

HGFPORTAL	Intranet server running Microsoft SharePoint™	Windows 2000 SP3
HGFWEB	Web server (IIS) providing internal application	Windows NT 4.0 SP6
HGFFILE2	File and print services	Windows NT 4.0 SP6
HGFEXCHANGE	Exchange 5.5 Server	Windows NT 4.0 SP6
HGFSQLSERVER2	SQL Server 2000 database due to replace SQL Server 6.5 database for internal application	Windows 2000 SP3
IRVBDC	BDC for HGFPROPERTIES domain providing local validation to Irvine Branch	Windows NT 4.0 SP4
IRVFILE	Local file and print server for Irvine branch	Windows NT 4.0 SP4
HAYBDC	BDC for HGFPROPERTIES domain providing local validation to Hayward branch	Windows NT 4.0 SP5
HAYFILE	Local file and print server for Hayward branch	Windows NT 4.0 SP5
ANABDC	BDC for HGFPROPERTIES domain providing local validation to Anaheim branch	Windows NT 4.0 SP6
ANAFILE	Local file and print server for Anaheim branch	Windows NT 4.0 SP6

Upgrade Methodology

One of the first steps in upgrading a Windows NT 4.0 domain is to make a decision about the type of upgrade to perform. Should the current domain be upgraded in place to Active Directory? Or maybe to a parallel Active Directory domain where you use the Active Directory Migration Tool (ADMT) to upgrade users, servers, printers, and so on, to the new Active Directory domain? HGF Properties decided to perform an in-place upgrade of the current domain, a decision that means the PDC must be upgraded.

This upgrade can happen in a couple of different ways. One way to upgrade would be to start with the member servers and upgrade all of them to Windows Server 2003. After upgrading the member servers, the domain controllers can be upgraded to install Active Directory. This approach allows administrators to get familiar with the upgrade process before upgrading the actual accounts database.

Another method is to upgrade the domain controllers first. After the domain has been moved to Active Directory, all the member servers can be upgraded. This approach is more useful if an organization is looking to gain the benefits of Active Directory as soon as possible. It also is useful when the need to upgrade to Active Directory is driven by an application. For example, an organization may need to upgrade a certain application, but its latest version requires Active Directory.

For this scenario, suppose HGFPROPERTIES has an Exchange 5.5 Standard Edition server with a 15.5 GB information store. This version of Exchange has a 16-GB limit on the information store. If HGFPROPERTIES wants to upgrade their server to Exchange 2000 Enterprise with a larger support information store, they must install Active Directory.

Server Upgrade Order

In this example, HGF Properties has decided to upgrade as many member servers as possible before upgrading the domain controllers. The next question is what servers to upgrade in what order. Some factors in this decision include:

- **Services running on the various servers.** How will the upgrade of a computer affect the services running on that computer? For example, after the domain is upgraded to Active Directory, DHCP servers need to be authorized before they give out addresses.
- **Number of users affected by upgrading a particular server.** Is there a server used by only a handful of users? If so, this may be a good candidate to upgrade before a server that affects the entire organization.
- **Application's dependency on Active Directory or other applications.** Is there a particular application being written or purchased that requires Active Directory? Are there any servers that may need to be upgraded together because of their dependencies on one another?
- **Server hardware.** Can the server hardware support Windows Server 2003? Most Windows NT 4.0 servers have 4 GB or smaller boot partitions. Is there enough space on this drive to support Windows Server 2003? Is the processor fast enough to do the job?

It is decided that all file and print servers will be upgraded first. That way, the company's administrators can start by upgrading computers that won't affect too many other functions. One of the main concerns during the upgrade is the print drivers. Research must be done to ensure the printers will work with the new operating system and that all clients can still access the printers after the upgrade. This task could be tested in a lab environment before the upgrade takes place. Also, remember that IRVFILE must be upgraded first to SP 5.0 before being upgraded to the new operating system.

The plan reveals that HGFSQLSERVER2 and HGFWEB essentially replace the functionality of HGFSQLSERVER, the SQL Server 6.5 database for an internal custom application. Because the migration to a new custom application is a process that will happen in the near future, it is decided that HGFSQLSERVER will not be upgraded. In fact, the hardware is out-of-date as well, so it is decided that the server will be retired after the application is upgraded in the next month or so.

HGFEXCHANGE poses a problem. If it is upgraded to Windows Server 2003, Exchange 5.5 will not work. The information store will fail to start after the upgrade. If Exchange 5.5 is upgraded to Exchange 2000 first, and then the server is upgraded to Windows Server 2003, the same thing will happen. Neither Exchange 5.5 nor Exchange 2000 is supported under Windows Server 2003.

At the time this guide was written, Exchange 2003 had not yet been released, so the server must keep Windows NT 4.0 or be upgraded to Windows 2000. If the computer is upgraded to Windows 2000, the Exchange server can be upgraded to Exchange 2000 as well. HGF Properties has decided to take a different approach. It has been decided that a new server will be purchased to act as the new mail server running Exchange 2000 and Windows 2000. Later, this server will be

upgraded to Windows Server 2003 and Exchange 2003. The hardware for the Exchange 5.5 server is still sufficient for other tasks and can be reassigned after Exchange is upgraded to the new server.

HGFWEB is tackled next. The current Web-based application is tested on a Windows Server 2003 server running IIS 6.0 in a lab environment. After any problems are solved, the server is upgraded to Windows Server 2003. HGFSQLSERVER2 is then upgraded from Windows 2000 to Windows Server 2003. HGFREMOTE runs Terminal Services on Windows 2000, so it becomes the next candidate for an upgrade. Finally, the portal server, HGFPORTAL, is upgraded from Windows 2000 to Windows Server 2003.

Active Directory Upgrade

Now that all the member servers have been upgraded, it is time to upgrade to Active Directory. To do this, the PDC must be upgraded first. One recommended approach is to use a new computer. By using a new computer, some of the risk of upgrading to Active Directory can be mitigated.

The administrators at HGF Properties first install the new server, called HGFDC1, as a Windows NT 4.0 BDC in the HGFPROPERTIES domain. Next, this new server is promoted to the PDC, a step that allows the original domain controller—now a BDC—to be promoted back to PDC status if something goes wrong during the upgrade. As an added precaution, the original PDC can be taken completely offline and reinstated after a successful upgrade.

This process affords the administrators a certain level of comfort knowing they can return the domain back to its original configuration in the event of an unsuccessful upgrade. The administrators would have performed normal backups of these computers before the upgrade process, so they actually have a couple of ways to get back to the original setup.

HGFDC1 is upgraded by inserting the Windows Server 2003 installation CD. The upgrade wizard automatically starts and the upgrade process is underway. The administrator must answer questions regarding the installation along the way as the operating system is upgraded to Windows Server 2003. Upon finishing the upgrade the server is rebooted and the administrator logs on to the new Windows Server 2003 system.

After the underlying operating system is upgraded, the Active Directory Wizard automatically starts. At this point Active Directory is still not installed but that is about to change. During the upgrade the administrators have to name the new Active Directory domain.

The name corp.hgfproperties.com is chosen as the internal domain name for Active Directory. Externally, HGF Properties is known as hgfproperties.com. This decision forces HGF Properties to run what is known as a split-brain DNS structure. Externally, they expose necessary computers and services using their external domain name. Internally, they maintain a completely different domain name. When the Active Directory wizard is complete and the computer is rebooted, Active Directory is installed and running.

What follows are some of the issues that HGF Properties administrators considered during their upgrade:

Forest Functional Level

During the upgrade process, the Active Directory installation wizard asks the installer to set the forest functional level. This setting is used to tell Active Directory how much backward compatibility to provide for other domain controllers. It is similar to the Windows 2000 mixed vs. native mode backward compatibility setting.

Active Directory Installation Wizard
Forest Functional Level
Choose the functional level of the new forest.
Set the forest functional level to Windows Server 2003 interim if your forest will not have any Windows 2000 domain controllers. This level allows Active Directory to efficiently manage large groups. It supports only Windows Server 2003 and Windows NT 4.0 domain controllers.
Choose the forest functional level:
Windows Server 2003 interim
For forests that will never have Windows 2000 domain controllers.
This change cannot be reversed.
Windows 2000
For forests that may have Windows 2000 domain controllers.
Note: both options allow the forest to have Windows NT 4.0 domain controllers.
< Back
Next >
Cancel

Figure 28. Choosing the forest functional level

The forest functional level allows an administrator to choose backwards compatibility with both Windows 2000 and Windows NT 4.0. The various options allow for fine-tuning the compatibility level by providing support for Windows 2000 domain controllers, Windows NT 4.0 domain controllers, or both simultaneously. Because this installation uses only Windows NT 4.0 domain controllers and no Windows 2000 domain controllers, the default option of Windows Server 2003 interim should be chosen.

DNS

Another issue that arises during the upgrade of the Windows NT 4.0 PDC to a Windows Server 2003 domain controller is DNS. The Active Directory installation wizard looks for a DNS server. If one is not found, the wizard prompts the user either to ignore the message and fix the problem after the install, install and configure a DNS server at that time, or allow the wizard to retest the connection to the DNS server. If this issue is not fixed during the installation, Active Directory does not function properly after the installation is complete.

Although not completely necessary, it is a good idea to use Microsoft DNS servers for Active Directory. Microsoft DNS supports all the necessary DNS services, such as SRV records and dynamic updates, required to run Active Directory efficiently. Various versions of BIND also offer enough support for Active Directory but don't offer Active Directory–integrated DNS. Active Directory integration offers the following benefits:

- Multimaster updates and enhanced security are based on the capabilities of Active Directory.
- Zones are replicated and synchronized to new domain controllers automatically whenever a new one is added to an Active Directory domain.
- Integrating storage of DNS zone databases in Active Directory streamlines database replication planning.
- Directory replication is faster and more efficient than standard DNS replication.

For more information on the benefits of Active Directory integrated DNS read the Help and Support center documentation in Windows Server 2003.

PDC Emulator

Now that the Windows NT 4.0 PDC has been upgraded to a Windows Server 2003 domain controller, the new Active Directory forest and domain run in Windows Server 2003 interim mode. This mode allows continued communication with the Windows NT 4.0 BDCs. In fact, the new Windows Server 2003 domain controller looks like a Windows NT 4.0 PDC to the BDCs. This computer is the first in the Active Directory domain, so it assumes all the FSMO roles. Remember, the PDC emulator role is the component that makes this server look like a PDC.

DHCP

Because the domain is now functioning as an Active Directory domain, services should be tested to make sure everything is functioning properly. One service of importance is the DHCP service. Only authorized DHCP servers are allowed to hand out TCP/IP addresses in Windows Server 2003. To test this, the **DHCP** administrator snap-in can be opened from **Administrative Tools** and the DHCP server added to the list of managed DHCP servers. If the server object displays a red arrow in the lower-right corner, the server needs to be authorized. This can be done by right-clicking the server object, and then clicking **authorize**. To see the change, the screen may need to be updated. Notice the options on the following screen.

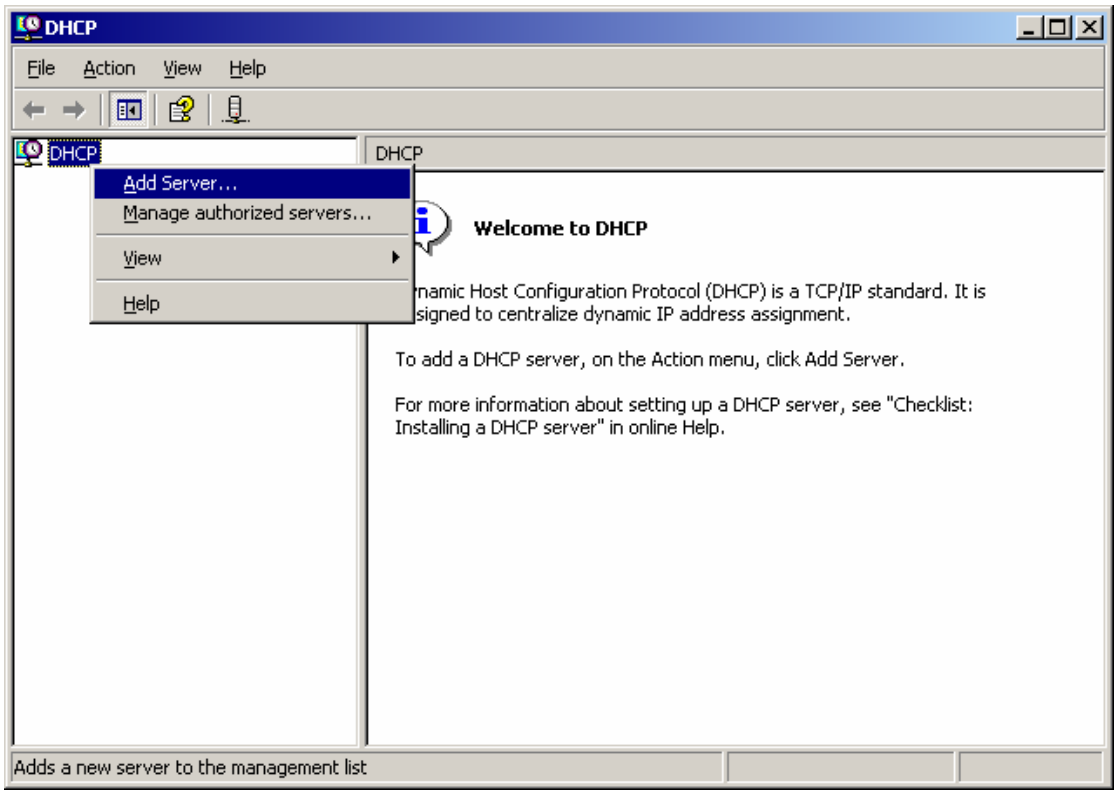

DHCP
File Action View Help
DHCP
Add Server...
Manage authorized servers...
View
Help
DHCP
Welcome to DHCP
namic Host Configuration Protocol (DHCP) is a TCP/IP standard. It is
signed to centralize dynamic IP address assignment.
To add a DHCP server, on the Action menu, click Add Server.
For more information about setting up a DHCP server, see "Checklist:
Installing a DHCP server" in online Help.
Adds a new server to the management list

Figure 29. DHCP Admin snap-in

WINS

The WINS service remains in place to support down-level clients. WINS filled the role of domain and computer locator service for previous versions of Windows NT. Windows Server 2003 does not require WINS in an environment without NetBIOS. However, WINS is always required in a mixed environment where Windows Server 2003–based computers interoperate with other systems, such as Windows NT 4.0, Windows 95, Windows 98, and Windows for Workgroups.

WINS Referral is the recommended way for Windows Server 2003 to address down-level computers registered in WINS. Because Windows Server 2003 resolvers are optimized to use DNS, they are much more efficient looking up down-level clients in a DNS database as opposed to WINS database. To enable this kind of lookup, a WINS referral zone can be created in DNS that points to the WINS database.

For example, the zone shown in the following dialog box does not perform any registrations or updates; it refers DNS lookups to WINS.

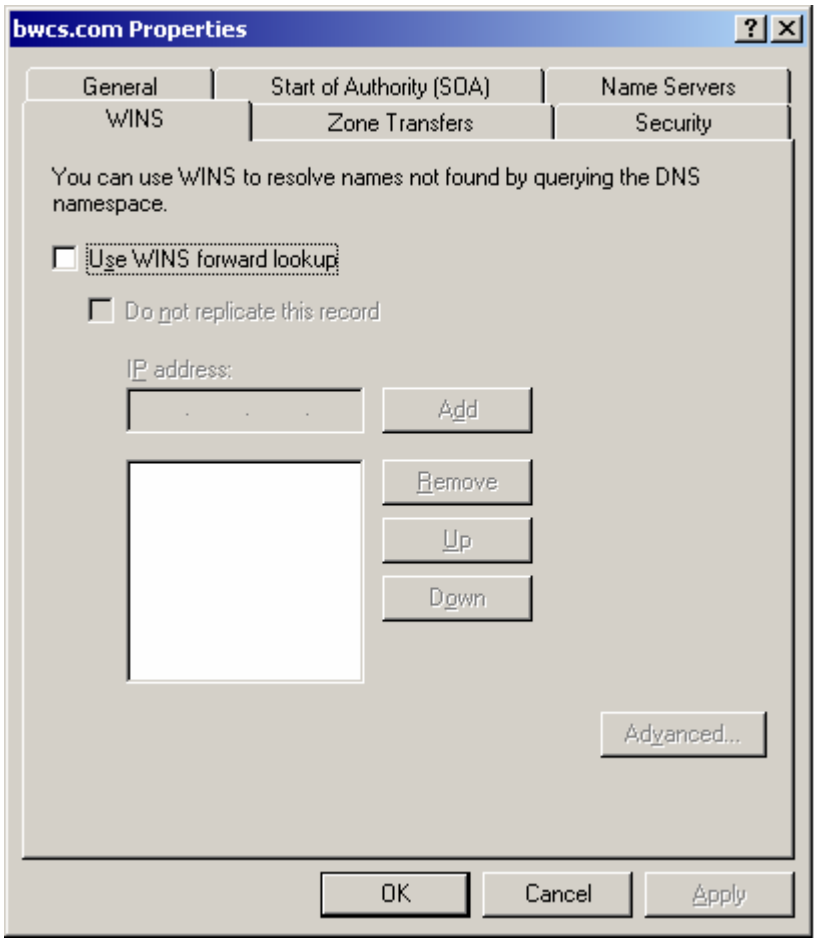


Figure 30. DNS WINS Referral tab

Whenever Windows Server 2003 servers or Windows XP–based clients send a query with an unqualified name (for example, *ntservermydomain*), the default domain name suffix is tried first. Additional suffixes, however, can be supplied as part of the DHCP configuration. If the name of the WINS referral zone is one of them, all WINS client names can be resolved.

For example, the figure below shows a WINS referral zone called *wins.mydomain.microsoft.com*, which has been created and directed to the WINS database.

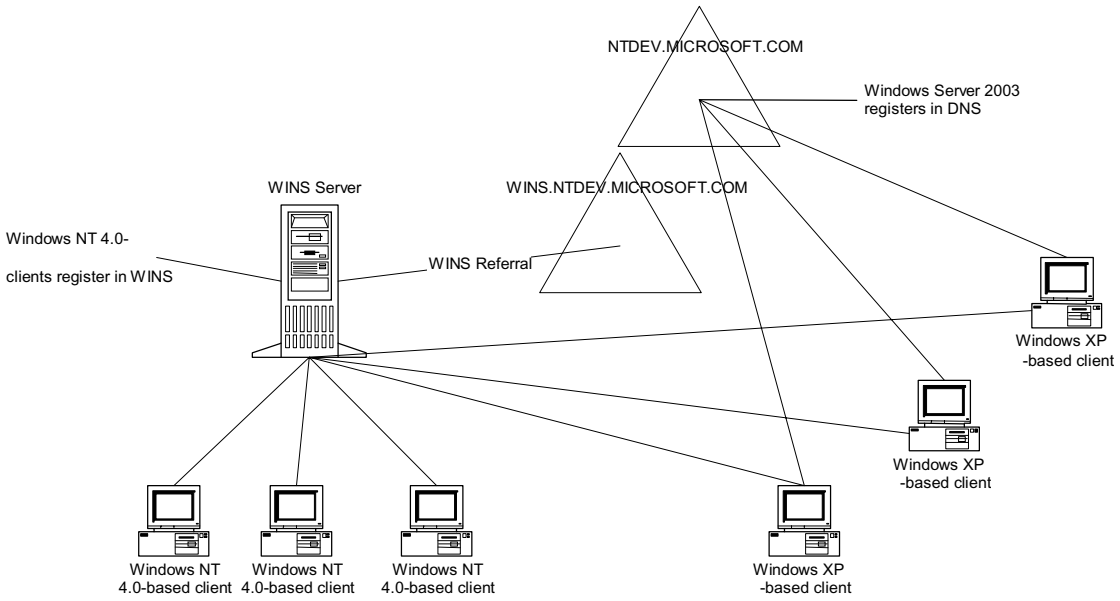


Figure 31. Resolution priority among referral zones

Figure 31 assumes that a Windows NT 4.0–based client has a name *client1*. A Windows XP-based client belongs to the *mydomain.microsoft.com.* If the Windows XP-based client has received a *wins.mydomain.microsoft.com.* suffix with its DHCP configuration, then in an attempt to resolve an unqualified name *client1*, it first tries the *mydomain.microsoft.com.* suffix (that is, *client1.mydomain.microsoft.com*). If that attempt fails, it tries *wins.mydomain.microsoft.com* (that is, *client1.wins.mydomain.microsoft.com*).

When the DNS server authorized for the *wins.mydomain.microsoft.com* zone receives the query, it cannot resolve the requested name. However, it is configured to use WINS lookup, so it submits a query for *client1* to the WINS server. The WINS server containing appropriate registration returns the host IP address to the DNS server, and then passes it to the Windows XP-based client.

HGF Properties has a few Windows NT 4.0 Workstation clients and even a few Windows 98 clients, so WINS is necessary until these clients are upgraded. When the WINS service is finally removed, it is a good idea to shut down the service first. That way, an administrator can watch the event logs for unexpected failures. If shutting down the service causes a failure, the problem can either be researched and solved, or the service can be turned back on. After the service has been shut down for a period of time and it seems as if no problems are noticed, the service can then be removed completely.

Remaining BDCs

Each of the five remaining BDCs needs to be upgraded. There are two BDCs in Los Angeles and one each in Irvine, Hayward, and Anaheim. The first two servers to upgrade are those in Los Angeles. It is decided to upgrade HGFBDC first, because it includes the WINS and DHCP services.

The server's name, HGFBDC, poses an interesting problem. After it is upgraded to a Windows Server 2003 domain controller, it is no longer a BDC. All domain controllers in Active Directory are

peer-to-peer using a multi-master relationship. The server name will be changed after the upgrade. Domain controllers can be renamed, but the domain must be running at the Windows Server 2003 functional level to support this ability.

Because the domain functional level is Windows Server 2003 interim, renaming the domain controller must wait. Once again, the domain functional level must be set to Windows Server 2003 before the name of a domain controller can be changed. The renaming procedure that follows is taken from the Help and Support Center in Windows Server 2003.

To rename a domain controller, follow these steps:

1. Open Command Prompt.
2. Type the following:

   netdom computername CurrentComputerName **/add:**NewComputerName

   This command updates the service principal name (SPN) attributes in Active Directory for this computer account and register DNS resource records for the new computer name. The SPN value of the computer account must be replicated to all domain controllers for the domain and the DNS resource records for the new computer name must be distributed to all the authoritative DNS servers for the domain name. If the updates and registrations have not occurred prior to removing the old computer name, then some clients may be unable to locate this computer using the new or old name.
3. Ensure the computer account updates and DNS registrations are completed.
4. Type the following:

   netdom computername *CurrentComputerName* **/makeprimary:***NewComputerName*
5. Restart the computer.
6. In Command Prompt, type the following:

   netdom computername NewComputerName **/remove:**OldComputerName

Value	Description
CurrentComputerName	The current, or primary, computer name or IP address of the computer you are renaming.
NewComputerName	The new name for the computer. The *NewComputerName* must be a fully qualified domain name (FQDN). The primary DNS suffix specified in the FQDN for *NewComputerName* must be the same as the primary DNS suffix of *CurrentComputerName* or it must be contained in the list of allowed DNS suffixes specified in the **msDS-AllowedDNSSuffixes** attribute of the **domainDns** object.
OldComputerName	The old name of renamed computer.

Renaming a domain controller requires that you first provide a FQDN as a new computer name for the domain controller. All of the computer accounts for the domain controller must contain the updated SPN attribute and all the authoritative DNS servers for the domain name must contain the host (A) resource record for the new computer name. Both the old and new computer names

are maintained until you remove the old computer name so that there is no interruption in the ability of clients to locate or authenticate to the renamed domain controller, except when the domain controller is restarted.

Note To perform this procedure, you must be a member of the Domain Admins group or the Enterprise Admins group in Active Directory, or you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.

To open a command prompt, click **Start**, point to **All Programs**, point to **Accessories**, and then click **Command Prompt**.

This command-line method requires Netdom, a tool installed with the Windows Support Tools in the Support\Tools folder on the Windows CD-ROM.

If the domain controller belongs to a group with a Group Policy enabled on its primary DNS suffix, the string specified in the Group Policy is used as the primary DNS suffix. The local setting is used only if the Group Policy is disabled or unspecified.

By default, the primary DNS suffix portion of a computer's FQDN is the same as the name of the Active Directory domain to which the computer is joined. To allow different primary DNS suffixes, a domain administrator can create a restricted list of allowed suffixes by creating the **msDS-AllowedDNSSuffixes** attribute in the domain object container. This attribute is managed by the domain administrator using Active Directory Service Interfaces (ADSI) or LDAP.

Domain controller locator (Locator) DNS resource records are registered by the domain controller after the renamed domain controller has been restarted. The records that are registered are available on the domain controller in the systemroot\System32\Config\Netlogon.dns file.

To enumerate the names with which the computer is currently configured, at a command prompt, type the following:

```
netdom computername ComputerName /enumerate:{AlternateNames | PrimaryName | AllNames}
```

You can also specify a parameter that uses administrator credentials required to modify the computer account in Active Directory. If this parameter is not specified, Netdom uses the credentials of the user currently logged on. For more information, see the Netdom command-line help.

If you rename a domain controller through the System Properties dialog box instead of using the Netdom tool, DNS and Active Directory replication latency may delay the ability of clients to locate or authenticate to the renamed domain controller. The length of this latency depends on your network design and the replication topology of your organization.

The Next Remaining BDC

The BDC called HGFPDC is upgraded next much like the other two domain controllers. Now there are three domain controllers at the Los Angeles location, but too few employees to justify maintaining them. The team wants to reduce the number of domain controllers and decides that PGFPDC will be demoted to a member server.

Keep in mind that PDCs and BDCs in Windows NT Server 4.0 can never be demoted. The administrator runs DCPROMO and performs the demotion process. After a server becomes a member server again, its name can be changed at any time.

Global Catalogs

The administrators use a similar procedure to systematically upgrade all remaining BDCs at the various locations. Each domain controller should also be configured as a global catalog server, which is a server that maintains a directory database queried by applications and clients needing to locate an object in a forest. The global catalog is hosted on one or more domain controllers and contains a partial replica of every domain directory partition in the forest. These partial replicas include replicas of every object in the forest, as Figure 32 shows: the attributes most frequently used in search operations and the attributes required to locate a full replica of the object.

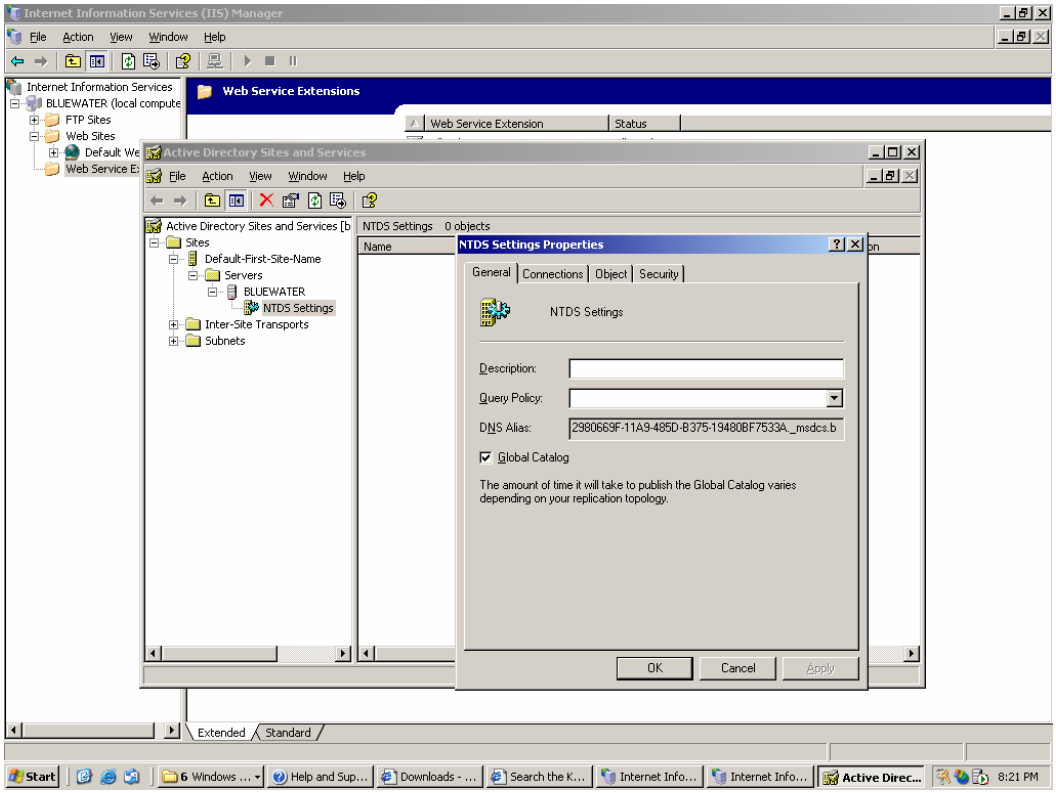


Figure 32. Global catalog settings

Results of the Upgrade

HGF Properties is now a long way toward completing their upgrade to Windows Server 2003 and Active Directory. Although there is more work to be done, such as upgrading the mail server to Exchange 2003 when it is released, the most challenging portions of the upgrade have been addressed.

Figure 33 shows the new Active Directory structure of the domain.

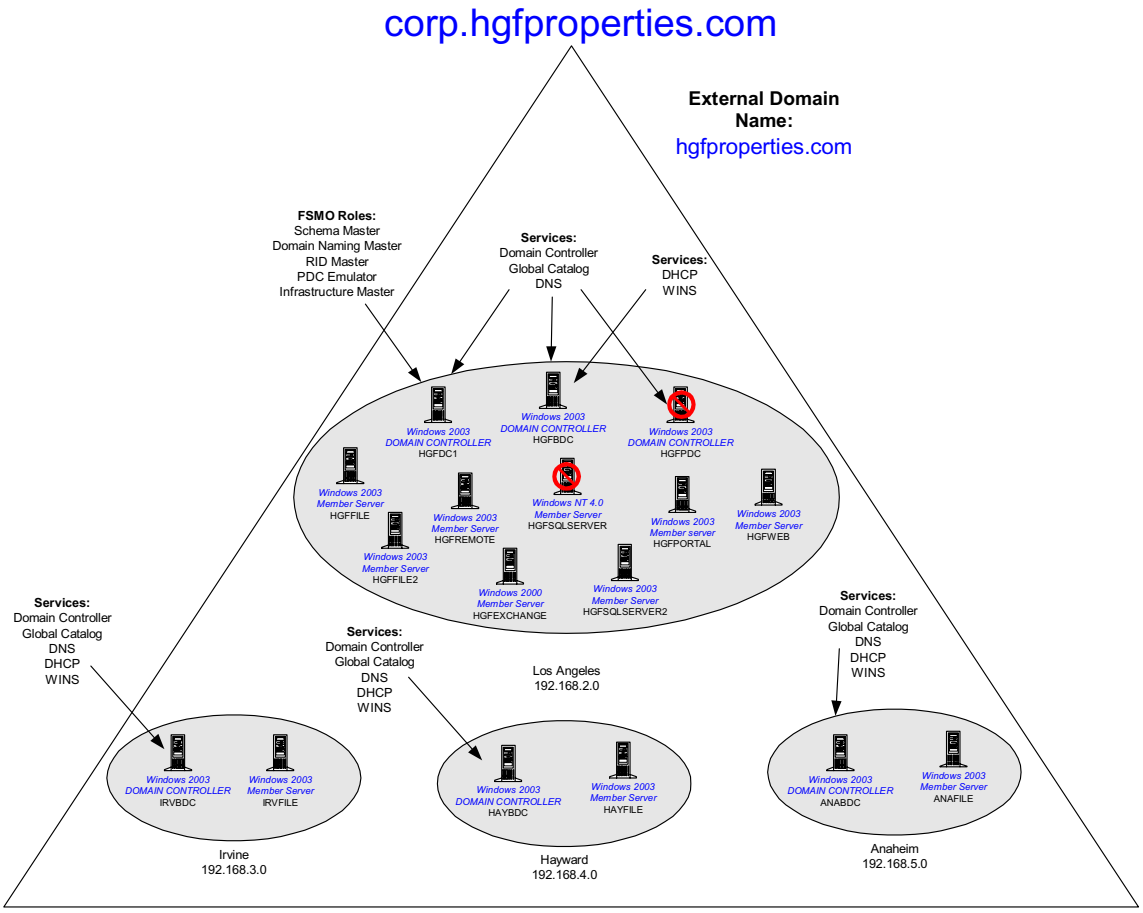


Figure 33. Upgraded server list

HGF Properties now has a single domain called corp.hgfproperties.com spread across four different locations. The table below lists the servers and their corresponding roles.

HGF Properties Servers and Roles After Upgrading

Server	Roles	Version
HGFDC1	§ Domain controller for Los Angeles and entire organization. If a domain controller fails in a remote office, the domain controllers in Los Angeles provide domain validation. § Schema master, domain naming master, RID master, PDC emulator, infrastructure master. § Global catalog. § DNS.	Windows Server 2003
HGFPDC	§ Domain controller for Los Angeles and entire organization § Global catalog § DNS	Windows Server 2003

HGFBDC	§ Domain controller for Los Angeles and entire location § Global catalog § DNS § Runs DHCP and WINS services	Windows Server 2003
HGFFILE	File and print services and Accounting server	Windows Server 2003
HGFSQLSERVER	SQL Server 6.5 database for internal custom application	Windows NT 4.0 SP6
HGFREMOTE	Remote access server running Terminal Services	Windows Server 2003
HGFPORTAL	Intranet server running Windows® SharePoint™ Services	Windows Server 2003
HGFWEB	Web server (IIS) providing internal application	Windows Server 2003
HGFFILE2	File and print services	Windows Server 2003
HGFEXCHANGE	Exchange 2000 Server	Windows 2000 SP3
HGFSQLSERVER2	SQL Server 2000 database due to replace SQL Server 6.5 database for internal application	Windows Server 2003
IRVBDC	Domain controller for HGFPROPERTIES domain providing local validation to Irvine Branch	Windows Server 2003
IRVFILE	Local file and print server for Irvine branch	Windows Server 2003
HAYBDC	Domain controller for HGFPROPERTIES domain providing local validation to Hayward branch	Windows Server 2003
HAYFILE	Local file and print server for Hayward branch	Windows Server 2003
ANABDC	Domain controller for HGFPROPERTIES domain providing local validation to Anaheim branch	Windows Server 2003
ANAFILE	Local file and print server for Anaheim branch	Windows Server 2003

Sample Upgrade Review

With most of the hard work done, HGF Properties now runs Active Directory, but some tasks remain to be planned or implemented. The upgrade team at HGF Properties still needs to address the following:

- Demoting a domain controller.
- Upgrading their internal business application.
- Changing computer names for old domain controllers.
- Planning their Exchange Server upgrade.
- Planning the eventual retirement of HGFSQLSERVER.

- Converting forest or domain functional level to Windows Server 2003.

Demoting a Domain Controller

HGF Properties already decided to remove one of the three domain controllers in Los Angeles. The upgrade team wants to demote one of them and repurpose it as a fax server.

They first select HGFPDC as the server to demote. Of the two original Windows NT 4.0 domain controllers, it provides the fewest services. By comparison, HGFBC runs the DHCP and WINS services. Rather than moving these services to another server, they decided to keep HGFBDC and demote HGFPDC. To demote HGFPDC, an administrator can either run DCPROMO or use the Configure Your Server tool, which can also start the DCPROMO utility.

After the wizard has successfully run, the server is rebooted and is no longer a domain controller. At this point the server is free to be repurposed.

Upgrading an Internal Business Application

The current Web-based business application interfaces with the SQL Server 6.5 database on HGFSQLSERVER. The application is being rewritten to use the new SQL 2000 server called HGFSQLSSERVER2. HGFSQLSERVER is the only computer left running Windows NT 4.0. It was decided that because the upgrade to the new application was almost complete, this server would not be upgraded. After the upgrade of the application to HGFSQLSERVER2 is complete, HGFSQLSERVER will be removed from the domain and retired.

Changing Computer Names for Old Domain Controllers

After HGFPDC is demoted to a member server, the administrators decide it to change its name before they repurpose it. The name is changed and the server is rebooted. At this point, the server is no longer a domain controller and no longer has the name of a former domain controller.

Keep in mind that the administrators still have a domain controller that needs to have its name changed. However, because it is a domain controller, it cannot have its name changed at the moment. The domain's forest functional level would need to be placed into Windows Server 2003 mode first. All domain controllers are now running Windows Server 2003, so this change can happen at any time.

However, the administrators want to make sure all is well before taking this irreversible step—they still need to retire the Windows NT 4.0 server running SQL Server. In addition, a number of Windows NT 4.0 Workstation–based computers and Windows 98–based computers also should be upgraded or retired. Although not necessarily a prerequisite, this assessment helps the team account for all down-level clients before turning on the final switch.

Planning the Exchange Server Upgrade

The team decided for now to upgrade their Exchange server to Exchange 2000. to do this, they could bring in new equipment and upgrade mailboxes to the new server or perform an in-place upgrade. By deciding to do an in-place upgrade, the server hardware does not have to change. The operating system must remain on Windows 2000, though, because Exchange 2000 does not

run on Windows Server 2003. It is decided to upgrade to Exchange 2003 at some time in the near future. Plans are already being made for that upgrade.

Planning the Eventual Retirement of HGFSQLSERVER

After the internal application that requires the data on HGFSQLSERVER has been updated to use the new server running SQL Server 2000, the original server can be retired. Again, the team will shut down the computer that is running SQL Server for a few days first just to make sure that its retirement causes no errors. If a problem arises, the server can be powered up and the problem can be fixed.

Part 2: Understanding Key Windows Server 2003 Components

Windows Services

There are many changes to services in Windows Server 2003. A service is a process, or set of processes, that offers basic and extended Windows functionality by providing support to programs at the system level. All services run in the background and are configured through the use of the service's application in Windows NT Server 4.0 or the services MMC snap-in in Windows 2000 and Windows Server 2003. For example, the World Wide Web (WWW) Publishing Service provides Web services and HTTP functionality.

Many of the changes to services in Windows Server 2003 were made to address security concerns and minimize the attack area for the default installation. Some services now run with lower permission than before; other services are not enabled by default, so you may need to enable them after installing Windows Server 2003.

New Services in Windows Server 2003

It's important to understand the default and extended services available in Windows Server 2003, because it helps you understand the functionality of a server more fully. In addition, you become better able to troubleshoot problems and enhance system security. For example, by disabling services that are not needed, you can help reduce a server's security exposure, reduce memory, and even provide for faster boot times.

To help reduce the default attack surface of Windows Server 2003, Microsoft disabled 19 services and reduced several services to run under lower privileges. For example, to help reduce the Web infrastructure attack surface, IIS 6.0 is not installed 0 by default when you install the operating system—you must explicitly select and install it. In addition, when IIS 6.0 is being installed, it is configured using its maximum security settings. After installation, IIS 6.0 accepts requests only for static files until configured to serve dynamic content, and all time-outs and settings are set to aggressive security defaults. IIS 6.0 can also be disabled using Windows Server 2003 group policies. For more information about IIS, see IIS 6.0 Security Changes later in this section.

Many of the ways in which these services are provided have changed from Windows NT Server 4.0 to Windows Server 2003. For a complete list of services and their functionality, see System Services for the Windows Server 2003 Family and Windows XP Operating Systems on the Microsoft TechNet Web site.

Setting Server Roles with the Configure Your Server Wizard

One important service change is the use of server roles. Using the Configure Your Server Wizard as Figure 34 shows, you can choose a type of server—that is, file server, application server, domain controller, or DNS server—and Windows Server 2003 automatically enables and disables the proper services for that role.

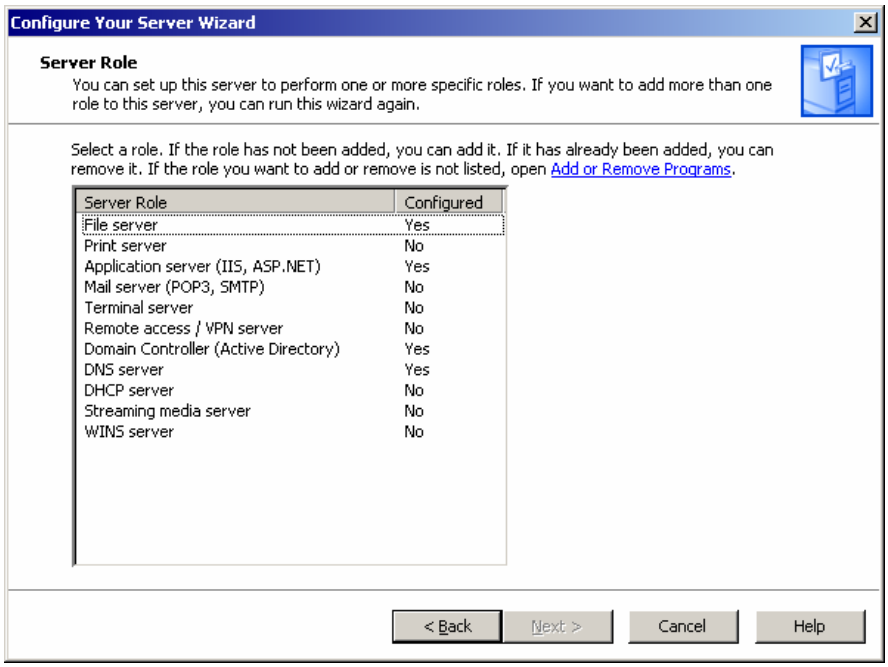

Configure Your Server Wizard
Server Role
You can set up this server to perform one or more specific roles. If you want to add more than one role to this server, you can run this wizard again.
Select a role. If the role has not been added, you can add it. If it has already been added, you can remove it. If the role you want to add or remove is not listed, open Add or Remove Programs.
Server Role
Configured
File server Yes
Print server No
Application server (IIS, ASP.NET) Yes
Mail server (POP3, SMTP) No
Terminal server No
Remote access / VPN server No
Domain Controller (Active Directory) Yes
DNS server Yes
DHCP server No
Streaming media server No
WINS server No
< Back
Next >
Cancel
Help

Figure 34. Configure Your Server Wizard

Starting and Stopping Services with the MMC

The Services applet in Windows NT 4.0 has been replaced in windows Server 2003 by the Services MMC snap-in (services.msccan), which is in the %systemroot%\system32 folder. You can use this snap-in to view and configure system services and for the following tasks:

- Start, stop, pause, resume, or disable a service on remote and local computers.
- Setup recovery actions in case of service failure. A service can be configured to behave differently on the first, second and subsequent failures.
- Enable and disable services per a certain hardware profile.
- Export service information to a .txt or .csv file for system administration purposes—use the Export List option from the Action menu.
- View the status, description, and dependencies of a service.
- View and change the security context of a service.

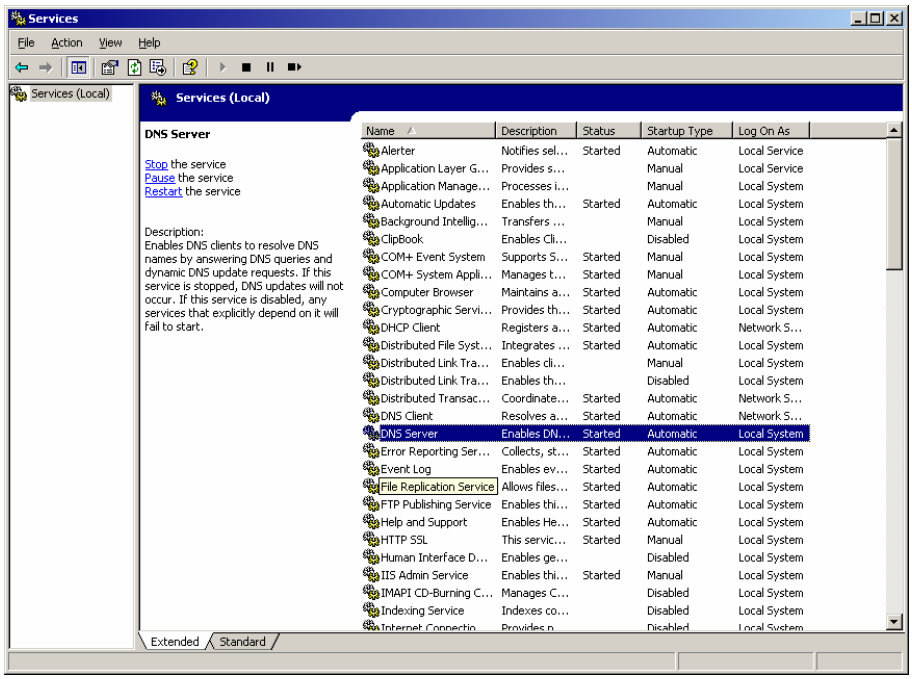

Services
File Action View Help
Services (Local)
Services (Local)
DNS Server
Stop the service
Pause the service
Restart the service
Description:
Enables DNS clients to resolve DNS names by answering DNS queries and dynamic DNS update requests. If this service is stopped, DNS updates will not occur. If this service is disabled, any services that explicitly depend on it will fail to start.
Name Description Status Startup Type Log On As
Alerter Notifies sel... Started Automatic Local Service
Application Layer G... Provides s... Manual Local Service
Application Manage... Processes i... Manual Local System
Automatic Updates Enables th... Started Automatic Local System
Background Intellig... Transfers ... Manual Local System
ClipBook Enables Cli... Disabled Local System
COM+ Event System Supports S... Started Manual Local System
COM+ System Appli... Manages t... Started Manual Local System
Computer Browser Maintains a... Started Automatic Local System
Cryptographic Servi... Provides th... Started Automatic Local System
DHCP Client Registers a... Started Automatic Network S...
Distributed File Syst... Integrates ... Started Automatic Local System
Distributed Link Tra... Enables cli... Manual Local System
Distributed Link Tra... Enables th... Disabled Local System
Distributed Transac... Coordinate... Started Automatic Network S...
DNS Client Resolves a... Started Automatic Network S...
DNS Server Enables DN... Started Automatic Local System
Error Reporting Ser... Collects, st... Started Automatic Local System
Event Log Enables ev... Started Automatic Local System
File Replication Service Allows files... Started Automatic Local System
FTP Publishing Service Enables thi... Started Automatic Local System
Help and Support Enables He... Started Automatic Local System
HTTP SSL This servic... Started Manual Local System
Human Interface D... Enables ge... Disabled Local System
IIS Admin Service Enables thi... Started Manual Local System
IMAPI CD-Burning C... Manages C... Disabled Local System
Indexing Service Indexes co... Disabled Local System
Extended Standard

Figure 35. Extended view in the Services snap-in

The applet located in Control Panel in Windows NT 4.0 has been removed in Windows Server 2003. As an alternative, use the shortcut located under Administrative Tools to access this snap-in. The Services snap-in in Windows Server 2003 offers two views of system services:

- The Extended view displays a description of a service and provides a button to stop, pause, and restart a service.
- The Standard view is similar to Windows 2000 and does not show the full description or offer the extra buttons for changing the status of a service.

To change the status of a service in Standard view, right-click a service to display options.

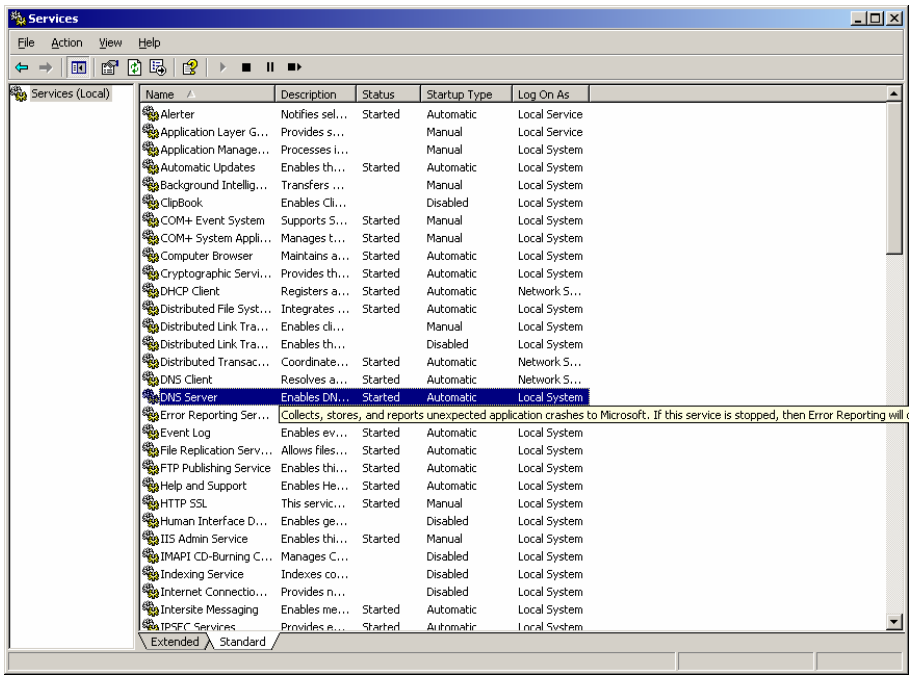

Services
File Action View Help
Services (Local)
Name Description Status Startup Type Log On As
Alerter Notifies sel... Started Automatic Local Service
Application Layer G... Provides s... Manual Local Service
Application Manage... Processes i... Manual Local System
Automatic Updates Enables th... Started Automatic Local System
Background Intellig... Transfers ... Manual Local System
ClipBook Enables Cli... Disabled Local System
COM+ Event System Supports S... Started Manual Local System
COM+ System Appli... Manages t... Started Manual Local System
Computer Browser Maintains a... Started Automatic Local System
Cryptographic Servi... Provides th... Started Automatic Local System
DHCP Client Registers a... Started Automatic Network S...
Distributed File Syst... Integrates ... Started Automatic Local System
Distributed Link Tra... Enables cli... Manual Local System
Distributed Link Tra... Enables th... Disabled Local System
Distributed Transac... Coordinate... Started Automatic Network S...
DNS Client Resolves a... Started Automatic Network S...
DNS Server Enables DN... Started Automatic Local System
Error Reporting Ser... Collects, stores, and reports unexpected application crashes to Microsoft. If this service is stopped, then Error Reporting will
Event Log Enables ev... Started Automatic Local System
File Replication Serv... Allows files... Started Automatic Local System
FTP Publishing Service Enables thi... Started Automatic Local System
Help and Support Enables He... Started Automatic Local System
HTTP SSL This servic... Started Manual Local System
Human Interface D... Enables ge... Disabled Local System
IIS Admin Service Enables thi... Started Manual Local System
IMAPI CD-Burning C... Manages C... Disabled Local System
Indexing Service Indexes co... Disabled Local System
Internet Connectio... Provides n... Disabled Local System
Intersite Messaging Enables me... Started Automatic Local System
IPSEC Services Provides e... Started Automatic Local System
Extended Standard

Figure 36. Standard view of the Services snap-in

Service Security Contexts

Windows NT Server 4.0 and Windows 2000 support a single, built-in account used for various services. All services in Windows NT Server 4.0 and Windows 2000 use either the LocalSystem account or a user-defined account typically referred to as a service account. Most user-defined service accounts created for various applications in Windows NT Server 4.0 are created with a high level of permissions, such as a domain administrator.

A common problem with service accounts is how to maintain a password that is as secure as possible for these accounts. Most Windows NT 4.0 administrators set the *password never expires* flag for service accounts to ensure that these accounts do not automatically stop working when the password expires sometime in the future. This common practice creates a large security hole in many Windows NT 4.0 domains. Most service accounts in Windows NT 4.0 had elevated permissions with passwords that rarely changed.

Unfortunately for some applications, such as Exchange Server 5.5, there is no alternative to using a separate, user-defined service account. Because of the authentication complexities across Windows NT 4.0 domains using Exchange 5.5 services, a user-defined service account was required. Windows 2000 and Active Directory provided the ability to use the LocalSystem account, rather than a user-defined service account for some applications. Exchange 2000 was designed to take advantage of this fundamental change in the LocalSystem account.

Windows Server 2003 takes the LocalSystem security context one step further. Two new built-in accounts offer lower privileges for running services. Now, instead of one built-in account, three built-in accounts offer various security contexts. The security context restricts the service to accessing the resources accessible to the specified account. The three built-in service accounts are:

- **LocalSystem**. The LocalSystem account is a predefined, local account set to provide extensive privileges on the local computer. It acts as the computer on the network. The name of the account is LocalSystem. This account does not have a traditional password.
- **LocalService**. The LocalService account is a predefined, local account set to use minimum privileges on the local computer and present anonymous credentials on the network. The name of the account is NT AUTHORITY\LocalService. This account does not have a traditional password.
- **NetworkService**. The NetworkService account is a predefined, local account set to provide minimum privileges on the local computer. It acts as the computer on the network. The name of the account is NT AUTHORITY\NetworkService. This account does not have a traditional password.

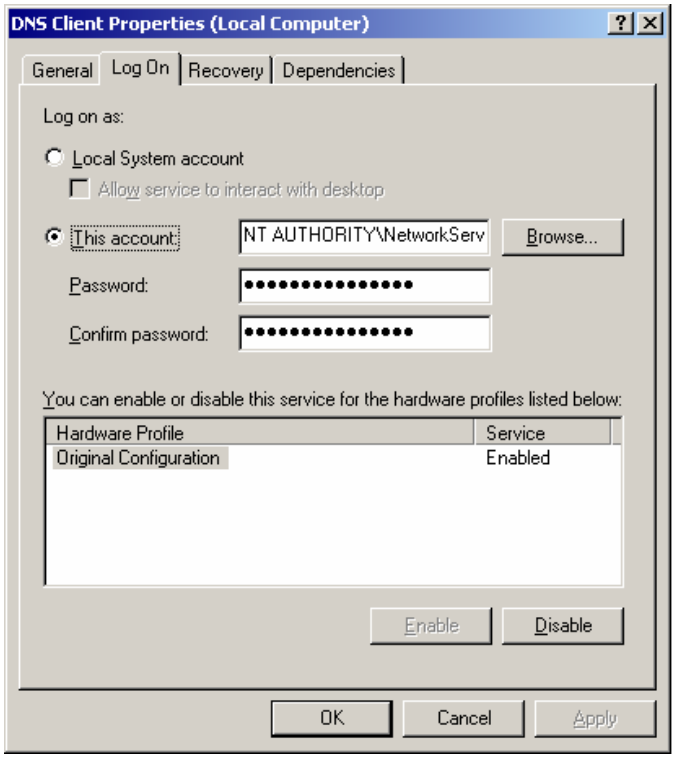


Figure 37. DNS Client Properties Log On tab

The three built-in accounts are designed for system activities and cannot be used for interactive access, unlike a user-defined service account, which can be used by anyone who has the password. The built-in accounts have no passwords to manage. Windows 2000 and Windows Server 2003 automatically change the password for the built-in accounts. The password is not based on a dictionary word, making it harder to hack. The resulting password is more secure than the values administrators typically generate, because the operating system randomly generates the password and automatically changes it on a frequent basis.

To find these accounts using Active Directory, open **Active Directory Users and Computers**. Make sure to enable **Advanced Features** using the **View** menu in this snap-in. Then open **ForeignSecurityPrincipals** to see a list of objects as Figure 38 shows. Expand the readable name field to see the human-readable names of these objects instead of the computer name.

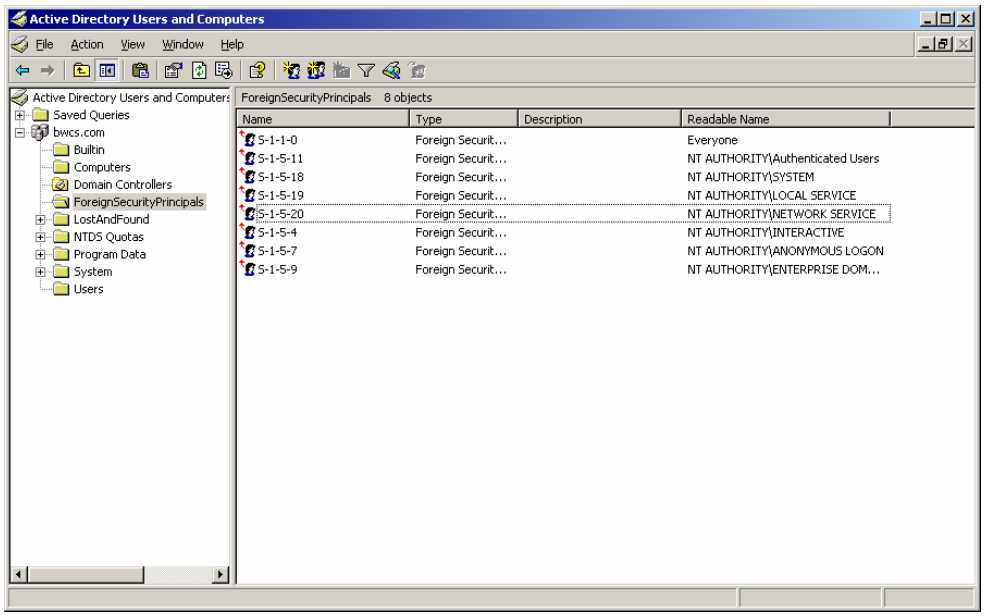


Figure 38. Active Directory User and Computers ForeignSecurityPrincipals

For more information about security, see Windows Server 2003 Security Guide on the Microsoft TechNet Web site.

Services Running Under Local Service

- Alerter
- Application Layer Gateway Service
- Remote registry
- Smart card
- Smart card helper
- SSDP Discovery Service
- TCP/IP NetBIOS helper
- Telnet
- UPS
- Universal Plug and Play
- Web client
- Windows Image Acquisition (WIA)
- WinHTTP Web Proxy Auto-Discovery Service

Services Running Under Network Service

- DHCP client

- Distributed Transaction Coordinator
- DNS client
- License logging
- Performance logs and alerts
- RPC locator

Services Disabled by Default

- IIS (not installed by default)
- Alerter
- Clipbook
- Distributed Link Tracking Server
- Human Interface Device Access
- IMAPI - CD Burning component
- ICF\ICS
- Intersite Messaging
- License logging
- Messenger
- NetMeeting Remote Desktop Sharing
- Network Dynamic Data Exchange (DDE)
- Network DDE and DDE share database manager (DSDM)
- Routing and remote access
- Telnet
- Terminal Service Session Discovery
- Themes
- Web client
- WIA
- The Kerberos KDC[3]

Svchost for Starting Services

Another change from Windows NT Server 4.0 to Windows Server 2003 is the use of the Svchost executable to start specific services. Svchost.exe is a generic host process name for services that are run from dynamic-link libraries (DLLs). The Svchost.exe file is located in the

[3] The Kerberos KDC is disabled by default, and then automatically enabled upon DCPromo.

%systemroot%\System32 folder. At startup, Svchost.exe checks the services portion of the registry to construct a list of services that it needs to load. Multiple instances of Svchost.exe can run at the same time. Each Svchost.exe session can contain a grouping of services so that separate services can run depending on how and where Svchost.exe is started. This flexibility provides better control and debugging.

Svchost.exe groups are identified in the following registry key:

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Svchost`

Each value under this key represents a separate Svchost group and appears as a separate instance when you are viewing active processes. Each value is a REG_MULTI_SZ value and contains the services that run under that Svchost group, as Figure 39 shows. Each Svchost group can contain one or more service_names extracted from the following registry key, whose Parameters key contains a ServiceDLL value:

`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Service`

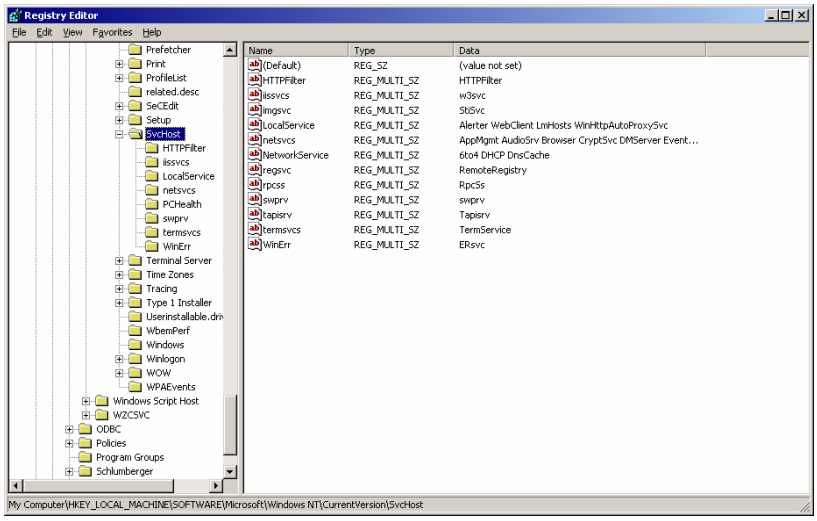


Figure 39. Svchost key in registry

It is helpful to know what processes are running on a computer. By opening the **Processes** tab in the **Task Manager** application, a list of currently running processes can be viewed. Typically more than one Svchost.exe process will be running on a healthy Windows Server 2003 server as Figure 40 shows. Through the use of these registry locations, you can understand the purpose of each instance of Svchost.exe.

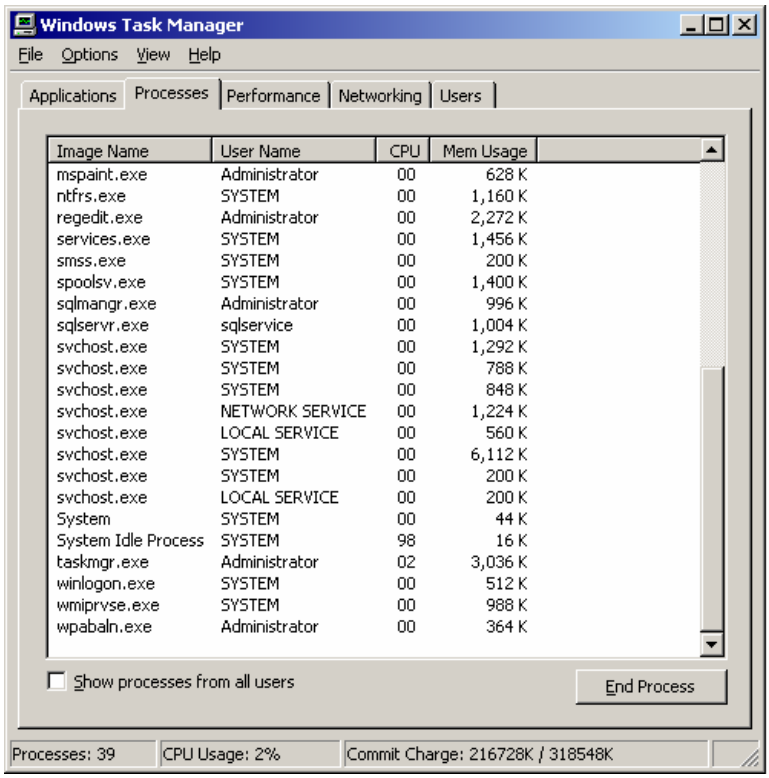

Windows Task Manager
File Options View Help
Applications Processes Performance Networking Users
Image Name User Name CPU Mem Usage
mspaint.exe Administrator 00 628 K
ntfrs.exe SYSTEM 00 1,160 K
regedit.exe Administrator 00 2,272 K
services.exe SYSTEM 00 1,456 K
smss.exe SYSTEM 00 200 K
spoolsv.exe SYSTEM 00 1,400 K
sqlmangr.exe Administrator 00 996 K
sqlservr.exe sqlservice 00 1,004 K
svchost.exe SYSTEM 00 1,292 K
svchost.exe SYSTEM 00 788 K
svchost.exe SYSTEM 00 848 K
svchost.exe NETWORK SERVICE 00 1,224 K
svchost.exe LOCAL SERVICE 00 560 K
svchost.exe SYSTEM 00 6,112 K
svchost.exe SYSTEM 00 200 K
svchost.exe LOCAL SERVICE 00 200 K
System SYSTEM 00 44 K
System Idle Process SYSTEM 98 16 K
taskmgr.exe Administrator 02 3,036 K
winlogon.exe SYSTEM 00 512 K
wmiprvse.exe SYSTEM 00 988 K
wpabaln.exe Administrator 00 364 K
Show processes from all users
End Process
Processes: 39
CPU Usage: 2%
Commit Charge: 216728K / 318548K

Figure 40. List of Svchost.exe processes in Task Manager

To view the list of services that are running in Svchost.exe on Windows Server 2003, type **Tasklist /svc** from a command line prompt. The **/svc** switch displays services hosted in each process. Type **Tasklist /?** to get a list of available switches as Figure 41 shows

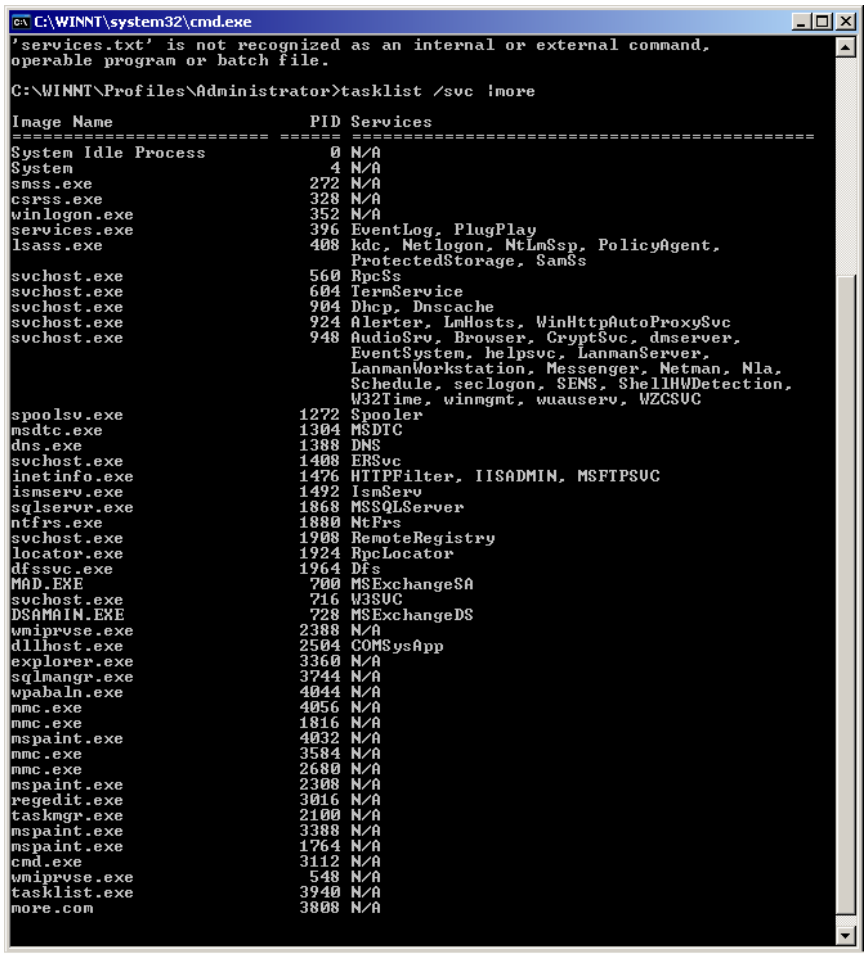


Figure 41. List of all services running in the Svchost.exe process

Security Changes Under Windows Server 2003

Windows Server 2003 is the first operating system to be launched under the Trustworthy Computing initiative. As a result, significant changes have been made to ensure that Windows Server 2003 is one of the most secure operating systems ever released by Microsoft. To make this commitment a reality many new features and changes have been added to the product.

Because Windows Server 2003 includes too many new features to list, the sections that follow discuss changes of particular interest to organizations that are migrating from Windows NT 4.0 Server. This section provides an overview of key differences in security-related features between Windows NT 4.0 and Windows Server 2003. In particular, changes to security-related features are discussed in more detail for IIS 6.0, COM+, the .NET Framework, authentication, access control, and network security.

Goals of the Trustworthy Computing Initiative

A short way of introducing the Trustworthy Computing initiative is to look at its goals, and then review the features and changes to Windows Server 2003 that help implement these goals.

The Trustworthy Computing Initiative considers trust from a user's point of view. The goals are designed to answer key user questions: Is the technology there when I need it? Does it keep my confidential information safe? Does it do what it's supposed to do? And do the people who own and operate the business that provides the technology always do the right thing? These are the goals that any trustworthy computing has to meet as the following table summarizes.

Trustworthy Computing Initiative Goals

Goal	Description
Security	The customer can expect that systems are resilient to attack and that the confidentiality, integrity, and availability of the system and its data are protected.
Privacy	The customer is able to control data about themselves, and those using such data adhere to fair information principles
Reliability	The customer can depend on the product to fulfill its functions when required to do so.
Business	The vendor of a product behaves in a responsive and responsible manner.

Microsoft has created a framework to track and measure its progress in meeting the security goals and objectives of the Trustworthy Computing initiative. For more information, see the Building a Platform for Trustworthy Computing white paper on the Microsoft Security Web site and Windows Server 2003 Security Guide on the Microsoft TechNet Web site.

IIS 6.0 Security Changes

Perhaps the biggest change in Windows Server 2003 is that IIS 6.0 is not installed by default. When IIS 6.0 is installed, ASP.NET support is enabled, but traditional ASP and ISAPI extensions are disabled by default.

If you are upgrading a Windows NT Server 4.0 computer, you will not see these security settings, because IIS is installed manually on Windows NT 4.0–based computers. You can continue to run existing ASP Web applications and other ISAPI extensions that you have enabled. By comparision, when upgrading a Windows 2000-based computer, IIS is installed by default but disabled; consequently, ASP and ISAPI extensions are disabled.

It is recommended that you do not upgrade but rather perform a clean installation of the operating system. After a clean installation, if you then install IIS, the Web Service Extensions are configured as Figure 42 shows.

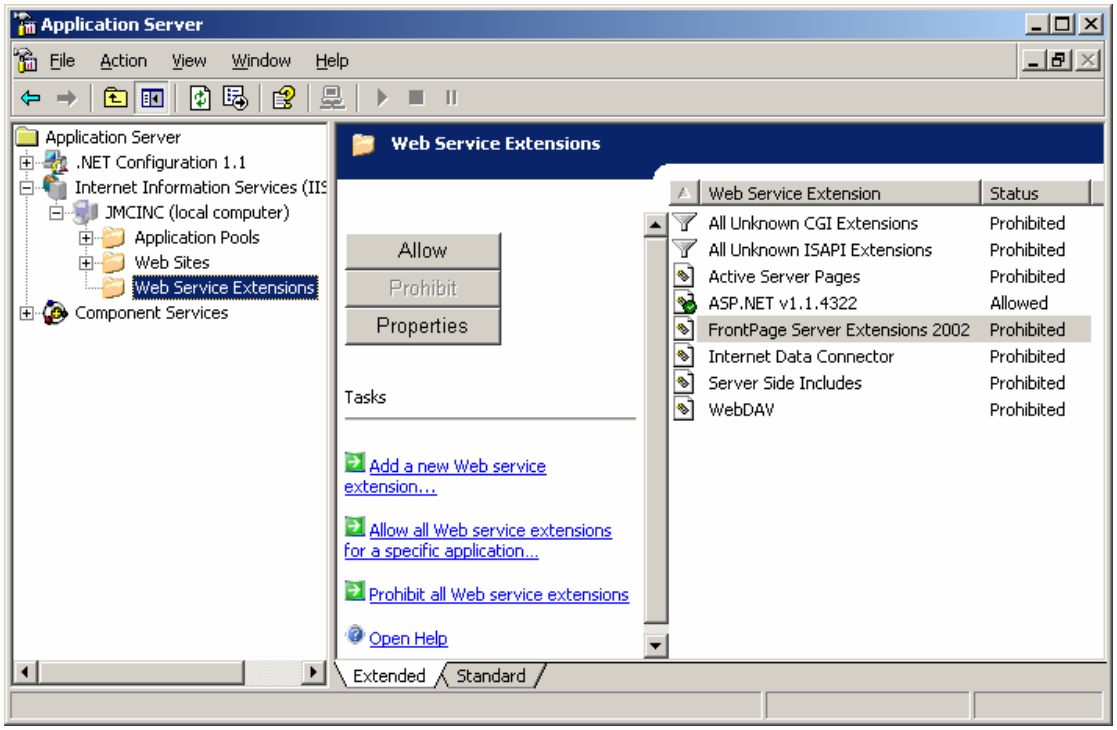


Figure 42. Default Web Service Extensions configuration folder in IIS 6.0

If you plan on running any earlier ASP applications, you should enable the ASP extension by using the same Application Server window.

IIS 5.0 Isolation Mode

Another significant security change in IIS 6.0 is its use of the following two isolation modes: IIS 5.0 isolation mode and worker process isolation mode. IIS 5.0 isolation mode keeps your computer as compatible as possible with older Web applications. It's designed to help applications that are dependent on the older memory model and process model of IIS 5.0 to run with success. This isolation setting should be used only as long as it takes to fix the compatibility issues with the

application. It is much less desirable than the newer worker process isolation mode described below.

IIS 5.0 isolation mode does not provide the ability to take advantage of application recycling or application pools. As Figure 43 shows, no Application Pools folder appears when a server is configured with IIS 5.0 isolation mode.

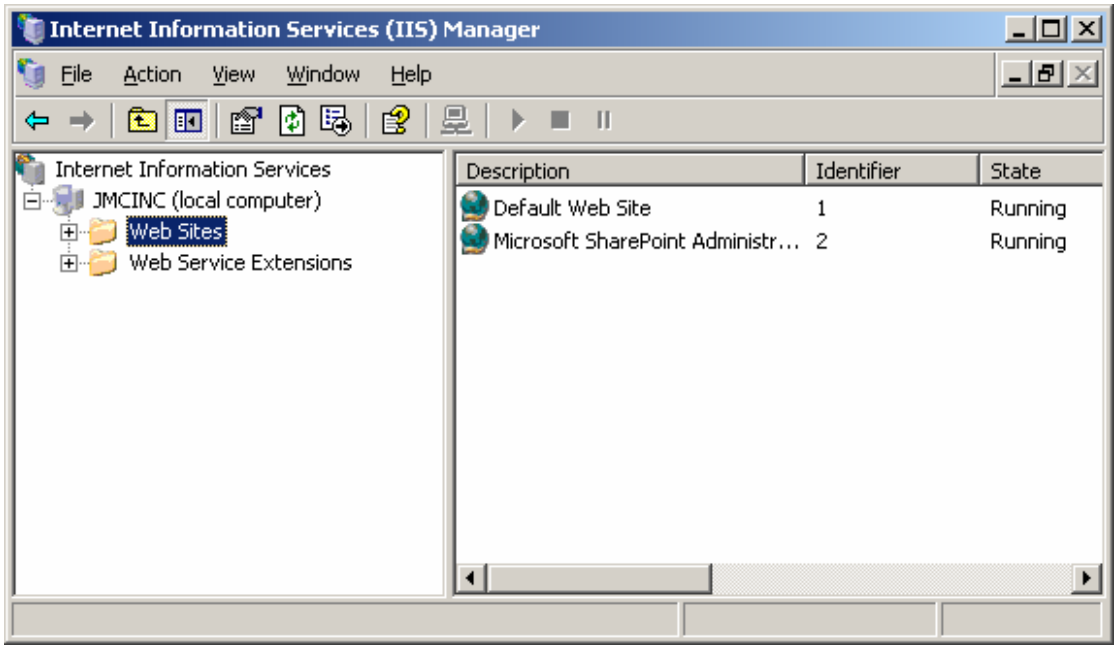


Figure 43. IIS 5.0 isolation mode

Worker Process Isolation Mode

Worker process isolation mode is the completely new, architected process model of IIS 6.0 and is the preferred setting on all computers. This mode allows you to run each virtual directory in its own isolated process if you want. In this mode, processes run under the NetworkService account by default instead of the LocalSystem account. The NetworkService account is granted far fewer rights. As a result, a system is less likely to become comprised when running in this mode.

In worker process isolation mode, you can change your identity to any one of the three built in accounts—LocalSystem, LocalService, NetworkService—or a user of your choice. If you create an account of your own, make sure that you add that account to the new IIS_WPG group, the group used by access control lists for IIS resources.

Configuring the IIS Isolation Mode

Figures 44 and 45 show the differences between the two isolation modes.

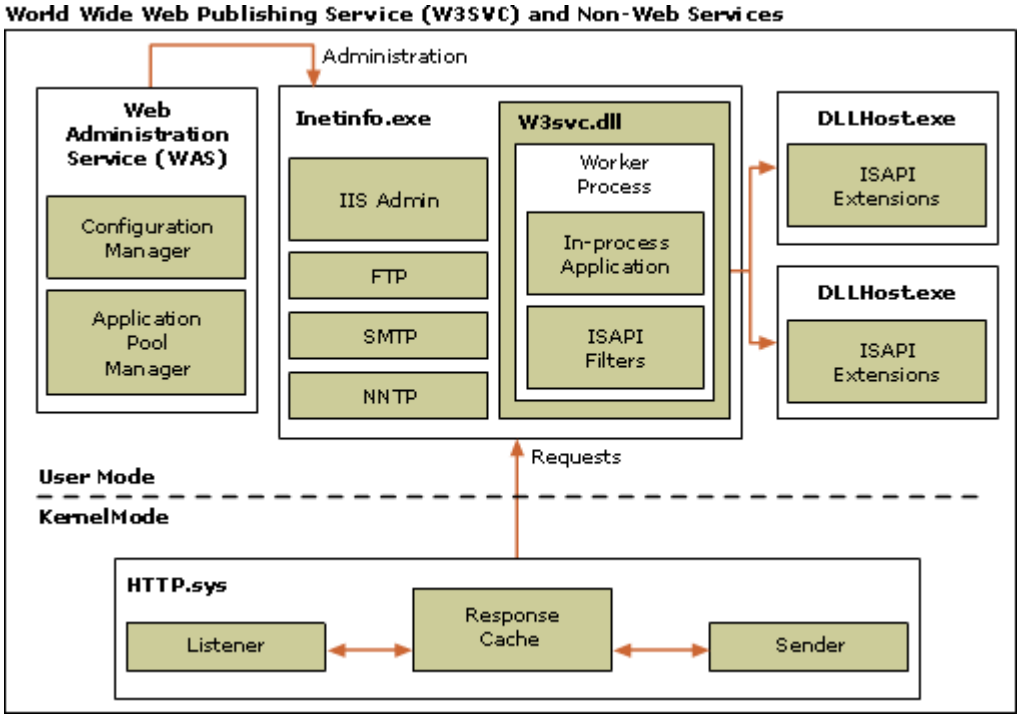


Figure 44. IIS 5.0 isolation mode

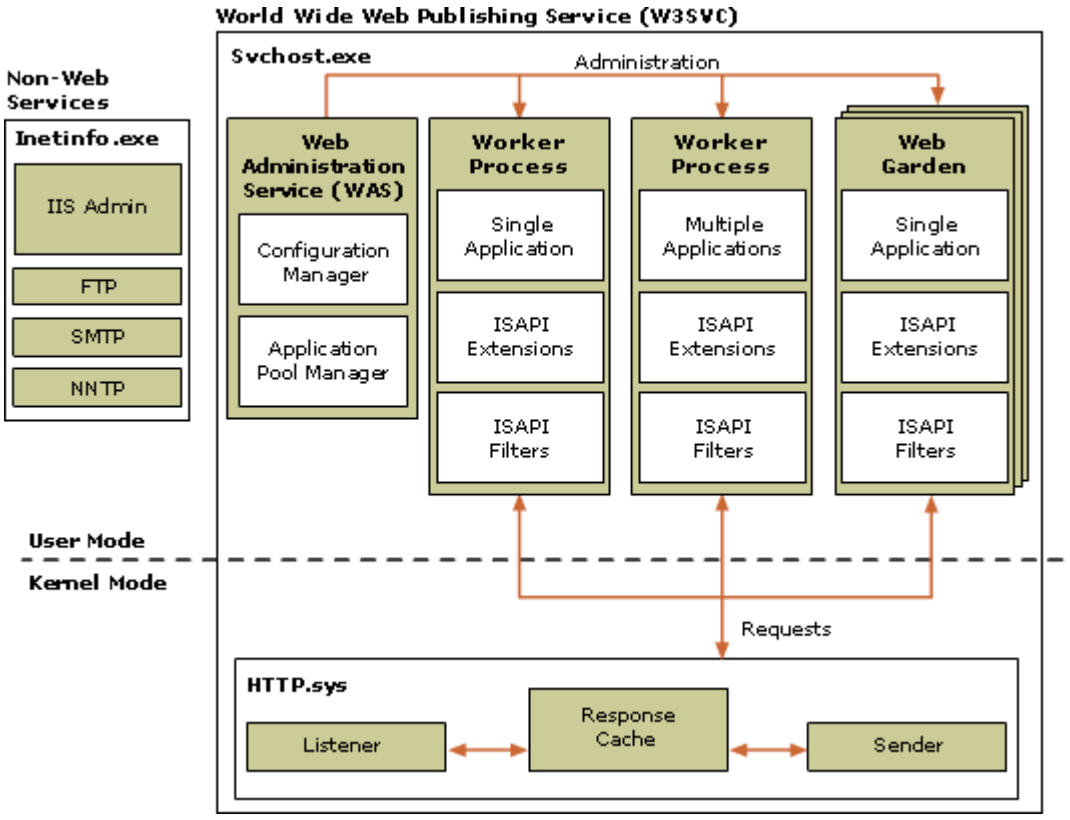


Figure 45. Worker process isolation mode

You cannot configure a computer to use both isolation modes at the same time. If you upgrade a computer from Windows NT Server 4.0 to Windows Server 2003, the IIS 5.0 isolation mode is used. You may want to switch to worker process isolation mode and verify that your applications are compatible with this setting. To do this, right-click **Web Sites**, select **Properties**, click the **Service** tab, and then click to clear the **Run WWW service in IIS 5.0 isolation mode** check box.

For more information about these modes, see the Internet Information Services (IIS) 6.0 section later in this guide.

New Security-Related Policy Changes

Root Access Control List (ACL)

A stronger ACL is set to stop access to the root directory (C:\). This change prevents non-administrators from modifying files created in off-root directories by other users. Stronger root ACLs also prevent users from writing files to the root directory, which is a known way to attack the operating system, because the root directory is in the system path. Users maintain the ability to create subdirectories of the root as well as the ability to create subdirectories and files in other users' directories. This concession is made for application compatibility. The ACL default share was also changed from Everyone Full Control to Everyone Read.

DLL Search Order Changed

Search order has been changed for DLLs. The current directory has been moved after system directories. This change affects only the applications that were using SetCurrentDirectory to load private versions of libraries found in system directories, such as %windir%\system32.

This setting was not safe for multiple threads nor even particularly necessary, because the directory from which an executable is launched is given preference anyway. Moreover, the setting may have opened up multiple-user and corporate networks to attacks based on spoofing system DLLs.

This change has been back ported to service packs for earlier systems, and no substantial compatibility problems have been reported.

Increased Restrictions on Anonymous Users

Anonymous users are no longer members of the Everyone group by default. On servers, Anonymous SID\Name translation is disabled; however, this setting is *not* disabled on the default on domain controllers. If your application made use of guest accounts, do extensive testing. Guest and anonymous users have been removed as a default member of the Everyone group. If your application requires guest access, you must explicitly give it.

Limits on Blank Passwords

Local accounts that have blank passwords cannot be used to connect remotely to a computer anymore.

Required Server Message Block (SMB) Packet Signing on Domain Controllers

This change provides integrity checking for client domain controller SMB communications and applies to Named Pipe Applications in particular.

By default, Windows Server 2003 domain controllers require that all clients digitally sign SMB-based communications. The SMB protocol is used to provide file sharing, print sharing, various remote administration functions, and logon authentication for some down-level clients. However, the following operating systems are not capable of performing SMB signing and therefore cannot connect to Windows Server 2003 domain controllers by default:

- Windows for Workgroups
- Windows 95–based computers without the DS Client Pack
- Windows NT 4.0–based computers prior to SP3
- Devices, including Pocket PC 2002 and previous versions, based on the Windows CE .NET version 4.1 or earlier

If such clients cannot be upgraded to a current operating system or upgraded to meet the minimum requirements described earlier in this article, then the SMB signing requirement can be removed by disabling the following security policy in the Default Domain Controller GPO on the domain controller's OU:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft Network Server: Digitally sign communications (always)
```

Warning Disabling this security setting exposes all your domain controller communications to "man in the middle" types of attacks. Therefore, it is highly recommended that you upgrade your clients rather than disabling this security setting. The DS Client Pack, necessary for Windows 95 clients to perform SMB signing, can be obtained from the \clients\win9x subdirectory of the Windows 2000 Server CD.

Required Secure Channel Communications

By default, Windows Server 2003 domain controllers require that all secure channel communications be either signed or encrypted. Secure channels are used by Windows NT–based computers for communications between domain members and domain controllers as well as among domain controllers that have a trust relationship. Windows NT 4.0–based computers prior to SP4 are not capable of signing or encrypting secure channel communications. If Windows NT 4.0–based computers prior to SP4 must join this domain, or this domain must trust other domains that contain pre-SP4 domain controllers, then the secure channel-signing requirement can be removed by disabling the following security policy in the Default Domain Controller Group Policy Object:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Domain Member: Digitally encrypt or sign secure channel data (always)
```

Warning Disabling this security setting exposes secure channel communications to "man in the middle" types of attacks. Therefore, it is highly recommended that you upgrade your Windows NT 4.0–based computers rather than disabling this security setting.

Modified LDAP Signing

This change affects the wldap32.dll LDAP bind initialization sequence so that signing is requested even if the client doesn't ask for it. This step does not occur if TLS or SSL protocol is used.

LSAP signing is similar in effect to the SMB signing. LDAP *always* requests signing now.

Stopped Allowed Paths Leakage

This change eliminates unnecessary information disclosure pertaining to system configurations. Many areas of the registry require Administrator privileges to read. However, security for certain branches was loosened through the use of the *AllowedPaths* key, which gave non-administrators privileges to read the data in that part of the registry. However, too much information could be read. Windows Server 2003 narrowed the paths to specific subtrees and specific subkeys. As a result, applications can no longer access a subtree around the data you are looking for.

Console Applications

Remote execution of console applications is now restricted to administrators only.

COM+ Security and Active Directory

Security in COM+ has been enhanced to integrate more closely with Active Directory by using two new technologies: COM+ partitions and partition sets.

COM+ partitions stored in Active Directory are used to map a local COM+ partition, which stores the actual COM+ application, to specific users or organizational units in your enterprise. COM+ applications are groups of COM components developed to work together to make use of COM+ services such as queuing, role-based security, and so on.

There are two types of COM+ partitions: COM+ partitions stored in Active Directory and local COM+ partitions stored on application servers. Using COM+ partitions stored in Active Directory, you can assign domain users and entire organizational units to applications stored in local COM+ partitions. Local COM+ partitions are application containers used to manage multiple instances of COM+ applications on a single application server.

A local COM+ partition can store only one instance of an application. For example, if you need to make two or more versions of the same application available to domain users, you must create two separate local COM+ partitions on an application server and associate (or link) them with two separate COM+ partitions in Active Directory.

To enable COM+ partitions, open **Component Services**, and then expand the list view to select a computer for which you want to enable partitions. Select **Properties**, click the **Options** tab, and select the **Enable Partitions** option. The following dialog box appears when enabling COM+ Partitions:

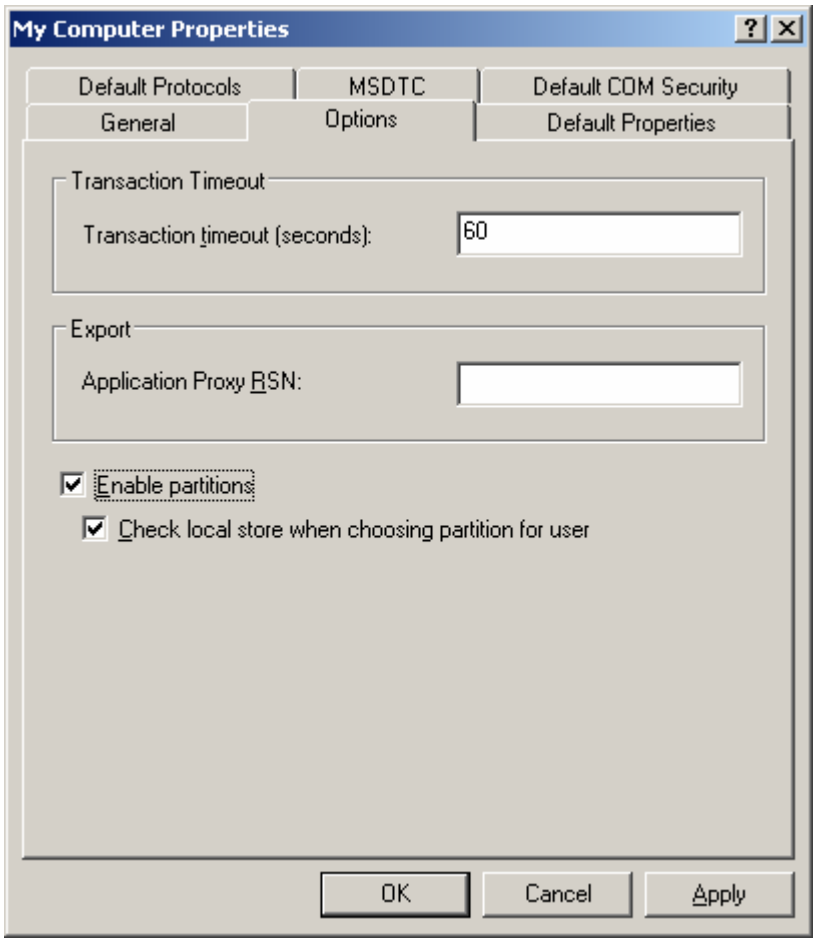


Figure 46. *Enabling COM+ partitions*

To learn more see “Managing COM+ Partitions in Active Directory” in the Help and Support Center installed with Windows Server 2003

Security Enhancements in the .NET Framework

The .NET Framework adds a new security model on top of the operating system security that you may be accustomed to. Before the .NET Framework, application developers and administrators focused on process-based security models instead of component-based security models. Process-based security models run all code with the same set of rights as the hosting process or thread that the code is actually running on. Component-based security models determine security based on information about the component, called *evidence*. This new model of component-based security is called *code access security* (CAS).

There are many types of evidence for a particular component, such as its author, its signature if signed, and its source (such as a local drive, a network share, or an URL). With the .NET Framework, the permissions with which a particular component runs are determined based on the evidence of a component and the permissions assigned to code groups found to have that evidence. The figure below compares the two security models.

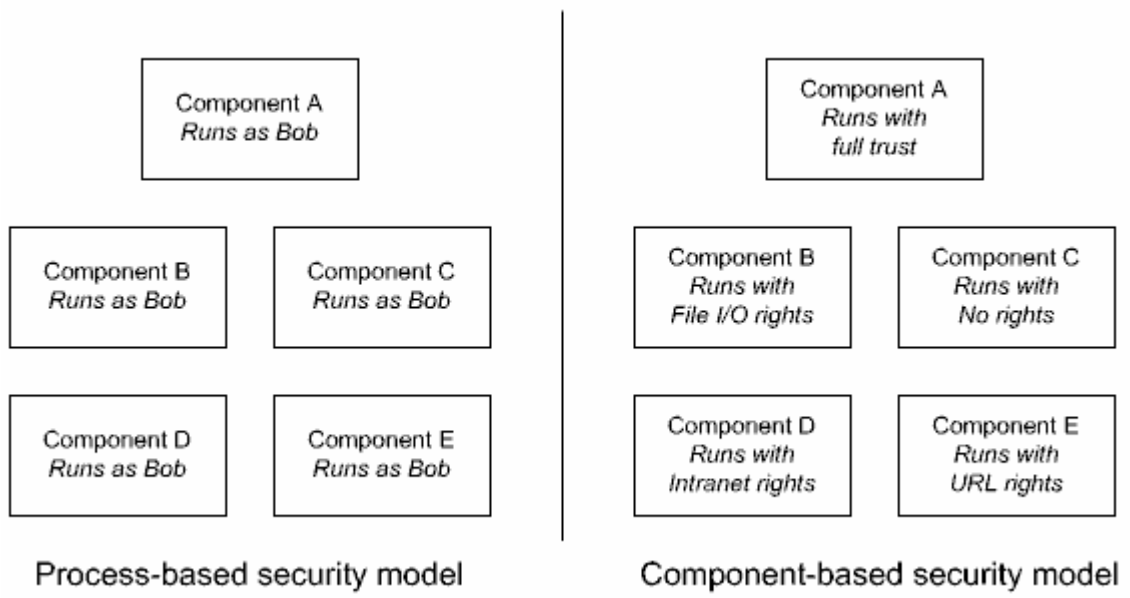


Figure 47. Comparing the Bob process under the earlier process-based security model and the new component-based security model in the .NET Framework

The new security model of the .NET Framework provides many features not available in a process-based model. One of the biggest advantages is the ability of the common language runtime to inspect a call stack during execution and verify that every assembly in the call stack has the rights to perform the requested task. Because the call stack is now inspected at runtime, an "untrusted" piece of code cannot lure a trusted piece of code into doing something. This security addition helps applications that are built using various component libraries from different vendors.

For more information about security, search for "security" in the .NET Framework Software Development Kit.

Security-Related Enhancements for Authentication

To authenticate local and remote users, Windows Server 2003 provides the following two new features of note:

- Credential Manager
- Constrained Delegation

Credential Manager

Credential Manager stores usernames and passwords and also stores links to certificates and keys. As a result, a consistent, single sign-on experience is provided for users—including roaming users. Single sign-on makes it possible for users to access resources over the network without having to repeatedly supply their credentials.

As an example, Credential Manager provides quick access to stored user names and passwords. To see this, open **Control Panel** and select **Stored User Names and Passwords** to display the following interface, which was designed to be intuitive to work with:

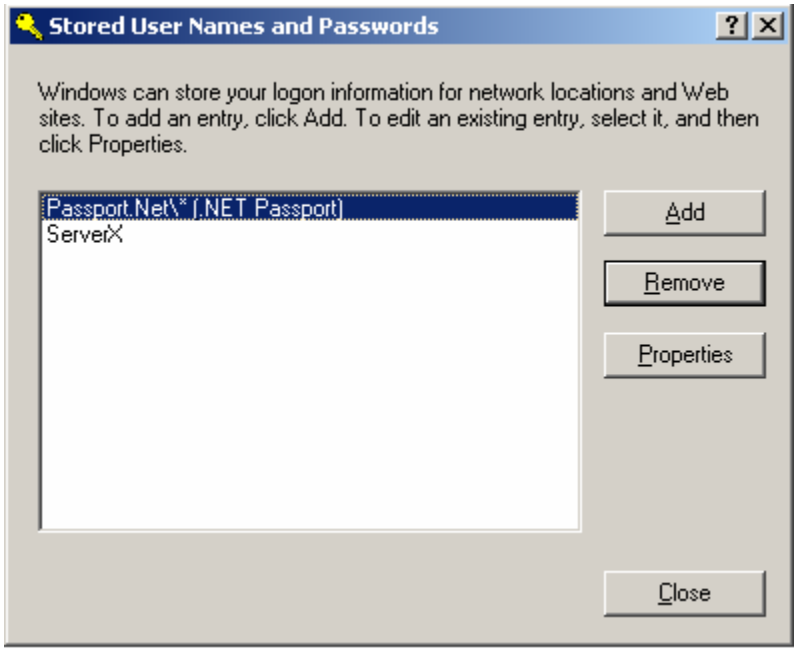

Stored User Names and Passwords
Windows can store your logon information for network locations and Web sites. To add an entry, click Add. To edit an existing entry, select it, and then click Properties.
Passport.Net* (.NET Passport)
ServerX
Add
Remove
Properties
Close

Figure 48. Stored User Names and Passwords dialog box

Constrained Delegation

Delegation is the act of allowing a service to impersonate a user account or computer account so that it can access resources throughout the network. Constrained delegation is a new feature in Windows Server 2003 that enables you to limit delegation to specific services and to control the particular network resources the service or computer can use. For example, a service that was previously trusted for delegation to access another computer on behalf of a user can now be constrained to use its delegation privilege only to that computer and not to other computers or services.

As an example of how constrained delegation works, open the **Active Directory Users and Computers** view, and then select **Computers.** Right-click a computer you want to trust for delegation, and then click **Properties**. Select the **Delegation** tab to display the following dialog box.

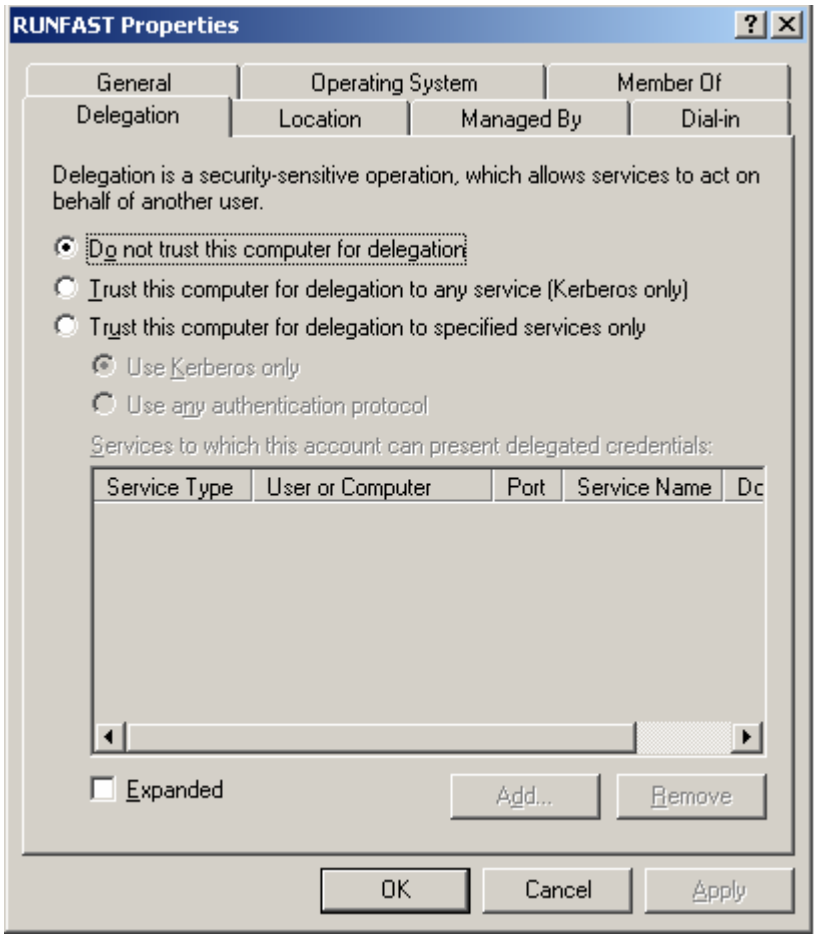


Figure 49. Delegation for specific services

Specify the settings you want for allowing delegation for a specific service, and you are finished.

If you do not see the delegation tab, make sure your computers functional domain level is set to **Windows Server 2003**. You can do this by opening **Active Directory Users and Computers**, right-clicking the domain, and selecting **Raise Domain Functional Level**. The dialog box shown in Figure 50 is displayed.

Important After you change your server's functional level to Windows Server 2003, you cannot change it back. By enabling this feature, you also enable all domain and forest functionality that is new in Windows Server 2003.

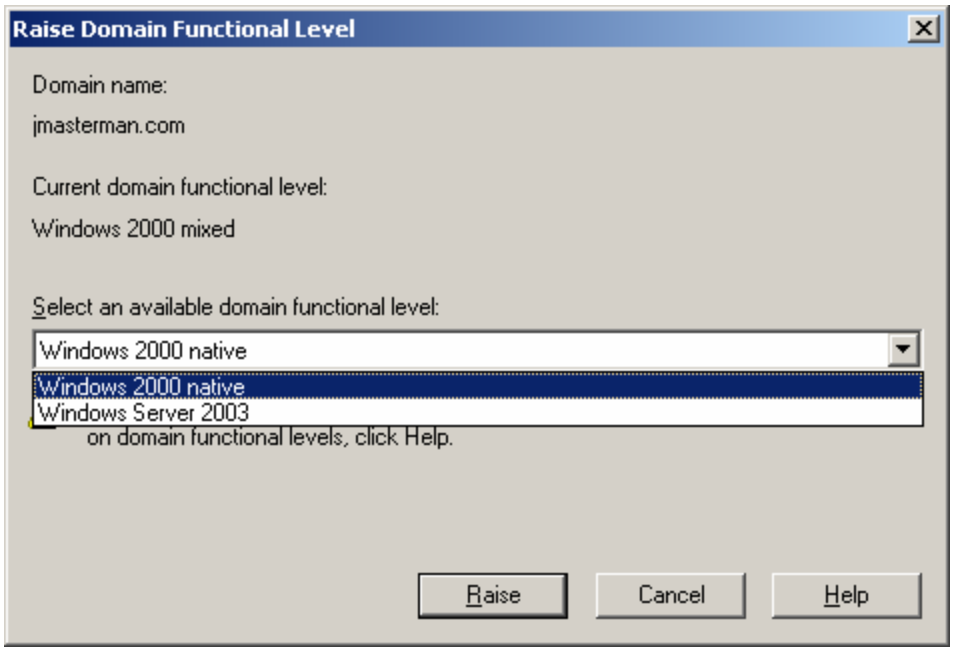


Figure 50. Raising the domain functional level

Security Enhancements for Access Control

Authorization can be used to help control access to resources by people, computers, and services. One very interesting example of this is software restriction policies. Network security is another, as the following sections describe.

Software Restriction Policies

Software restriction policies enable you to control execution of an application on a system. With this feature you can prevent applications from running on computers in your enterprise. To work with software restriction policies, you must first install the Windows Server 2003 Administration Tools Pack, which can be found on the Windows Server 2003 CD in the I386 folder. The installation file you need to run is Adminpak.msi.

Note Before installing the Administration Tools Pack, close all MMC applications.

After installing the Administration Tools Pack, run Mmc.exe. You must select the **Add/Remove Snap-In** option, and then select the **Group Policy Object Editor**. This step enables you to expand the tree view to add policies as Figure 51 shows.

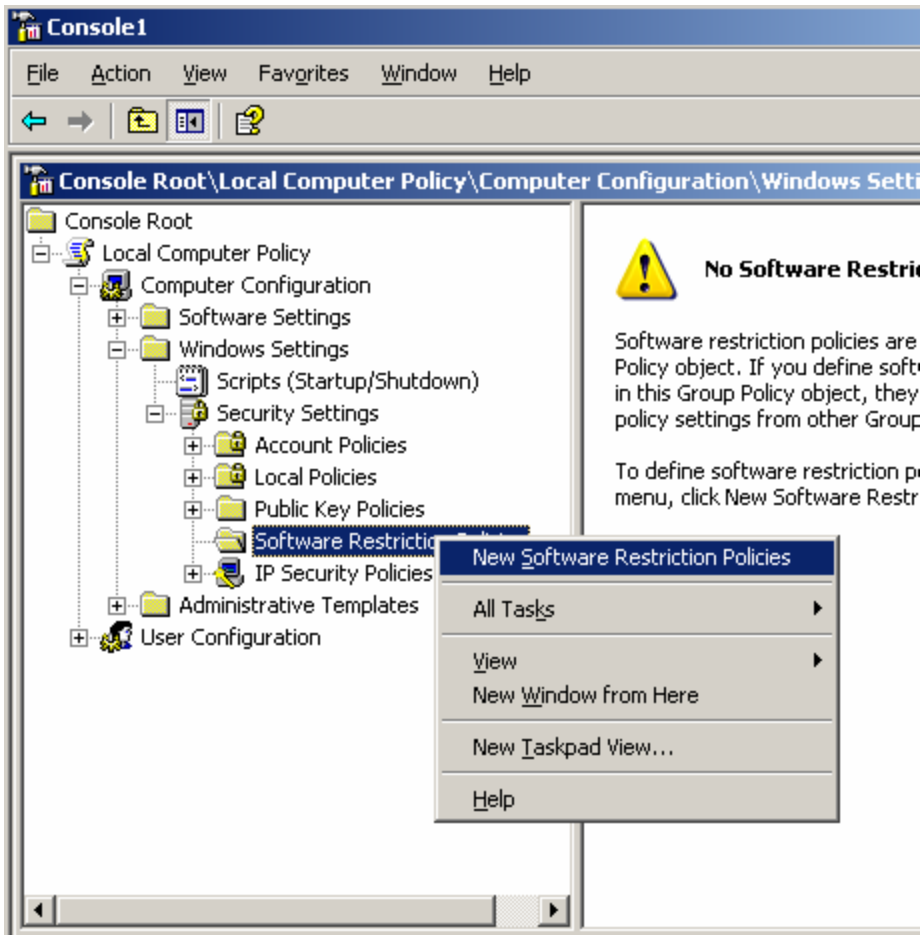


Figure 51. Adding software restriction policies through the Group Policy Object Editor

Network Security

With the popularity of wireless devices, the need for security in 802.1X networks is greater than ever. Users are increasingly mobile in today's workplace, and many users need to connect to the enterprise remotely. Windows Server 2003 has added the ability to inspect a remote computer's configuration before giving access to a private network. This option can be used to ensure that a remote computer has current services packs and appropriate updates before being allowed onto the network.

802.1X

Wireless security is a mandatory feature for most organizations today. With mobile users roaming the halls and connecting to enterprise resources from anywhere in the building, securing the communication is a necessity. Windows Server 2003 provides an easy mechanism for administering policy over wireless connections.

Quarantine

IAS Network Access Quarantine Control provides phased network access for remote client computers by restricting them to a quarantine mode. After the client computer configuration is either brought into or determined to be in accordance with your organization's network policy, quarantine restrictions, which consist of Quarantine IP-Filters and Session Timers, are removed and standard remote access policy is applied to the connection.

TCP/IP and Support for Earlier Networking Protocols

Today, TCP/IP is the dominant networking protocol suite in enterprise networks and across the Internet. When Windows NT 4.0 was first made available, this was not the case. This section describes the networking protocols no longer supported in Windows Server 2003 so that you can identify areas where you may encounter difficulty because of features that are no longer supported.

Before the global growth and popularity of the Internet, various networking protocols were used in networked environments, and the choice of protocol was often based on the size of the network or the expertise of the IT networking staff. With today's global Internet, linking even the smallest networks to the rest of the world, networking protocol expertise in TCP/IP is essential for networking professionals. TCP/IP is the networking protocol of choice. As a result, many other networking protocols have become obsolete.

With so many applications supporting TCP/IP, the protocols outlined in this section should present little difficulty for most applications and systems when upgrading. This information was compiled from various sources, including Microsoft Knowledge Base articles.

NetBEUI

Microsoft has removed support for the NetBIOS Extended User Interface (NetBEUI) network protocol in Windows Server 2003. However, some NetBIOS calls remain to assist with application compatibility. These interfaces are no longer tested and Microsoft cannot guarantee the level of functionality. It is recommended that you change your application’s NetBEUI-specific calls to corresponding NetBIOS calls and run it over another network protocol, such as TCP/IP or IPX.

Data Link Control (DLC)

Support for the Data Link Control (DLC) protocol has been discontinued in Windows Server 2003 and is not available to install.

The DLC protocol is primarily used for connectivity in IBM SNA environments for mainframes and minicomputers such as the AS/400. The DLC interface is most commonly used by 3270 terminal emulators to communicate with IBM mainframes. The functions that are performed by this protocol include error detection (by using a check character), error correction (by using time-outs and retransmissions), flow control (by using delayed acknowledgments and "receiver not ready" response frames), and the ability to have multiple devices on the same media (by using polling and acknowledgments).

DLC drivers that are available for Windows XP may also run on Windows Server 2003. A DLC driver for Microsoft Windows XP is available in Host Integration Server 2000. For more information, visit http://www.microsoft.com/hiserver. A Windows XP version of the DLC protocol is available as a free download from the Microsoft Download Center at http://www.microsoft.com/downloads

Important The Windows XP version of the DLC protocol is provided as is. The DLC protocol may not work properly with Windows Server 2003, it has not been tested, and Microsoft does not support the DLC protocol with Windows Server 2003.

An alternative is to find a third-party binary, such as one from IBM for DLC available from their Web site.

Quality of Service and RSVP Signaling

RSVP signaling has been completely removed from Windows Server 2003. Windows Server 2003 also removes the QoS Admission Control Service (ACS) component.

ACS no longer exists on Windows Server 2003. The RSVP service still runs on the host as a conduit between program and traffic-control components. However, no RSVP messages are generated.

GQoS programs can mark packets without ACS policy approval. Note that traffic-control programs can mark packets on Windows 2000, Windows XP, and Windows Server 2003. Earlier programs that use the IP_TOS socket option can mark packets on Windows NT 4.0. Administrators must manage these types of programs in their networks appropriately for their network and program requirements.

Dial-in Support: IPX and AppleTalk

Neither IPX nor AppleTalk (ARAP) are supported for dialing into Windows Server 2003–based computers.

Streams

Support for Streams, popular on the UNIX operating system and used for transport drivers, has been removed from Windows Server 2003.

Part 3: Application Compatibility Considerations

Internet Information Services (IIS) 6.0

IIS 6.0 is a complete Web server available in all versions of Windows Server 2003. With IIS 6.0, organizations of all sizes can quickly and easily deploy powerful Web sites and applications. IIS 6.0 provides a high-performance platform for applications built using the .NET Framework. Through IIS 6.0, organizations can also benefit from opportunities for server consolidation as well as reduced system downtime. Compared to earlier versions, IIS 6.0 improves Web site and application availability, helping organizations to lower system administration costs while improving Web server security.

Upgrading to IIS 6.0 provides other advantages as well. IIS 6.0 features a new fault-tolerant process architecture with health monitoring that runs all application code in an isolated environment for maximum dependability and availability. Web server administration is simplified using an XML-based configuration file that can be modified without having to stop and restart the server. IIS 6.0 enhancements, such as kernel-mode caching and processor affinity, dramatically increase the scalability and performance compared to previous versions of IIS. In addition, IIS 6.0 is not installed by default with Windows Server 2003 and is first installed with the highest security settings to help reduce the attack surface area.

This section discusses the IIS 6.0 features that have the greatest impact on server consolidation in the following areas:

- Features that increase the reliability of the overall Web application architecture and the availability to users of Web sites and applications hosted on that architecture.
- Manageability features that simplify Web server administration, whether script-based or GUI-based.
- Scalability features that maximize the use of existing and planned hardware technologies and capabilities.
- Security features that help reduce the vulnerability to attack and help provide security in building and deploying Web applications.

IIS 6.0 Reliability and Availability

IIS 6.0 has been completely redesigned with a new fault-tolerant process architecture that boosts the reliability of Web sites and applications. In previous versions of the product, the failure of a single Web application might cause the failure of other Web sites and applications on the same server. IIS 6.0 isolates Web sites and applications into self-contained units called *application pools*, separate from the other applications that are hosted on the same server. One or more distinct Windows *worker processes* serve each application pool. Worker processes operate independently, so if they fail, they do not affect other worker processes. The pooling of applications protects them from the effects of worker processes that support other application pools and protects each application from the other. The fault-tolerant architecture of IIS 6.0 increases the overall reliability of a Web server infrastructure, increases the availability of Web sites and applications, and increases the number of separate Web sites and applications that can run on a single server.

Several other IIS 6.0 performance and reliability features enable Web server consolidation, including the following:

- **Health monitoring.** IIS 6.0 periodically checks the status of an application pool and automatically restart it if Web sites and applications within that pool fail. As a result, application availability and overall Web infrastructure reliability are increased.
- **Application pools.** IIS 6.0 application pools are a convenient means of administering a set of Web sites and applications. Application pools increase reliability, because errors in one application pool cannot cause another application pool—or the server itself—to fail.
- **Automatic process recycling.** IIS 6.0 automatically stops and restarts faulty Web sites and applications based on a flexible set of criteria—including CPU utilization and memory consumption—while queuing requests.
- **Rapid-fail disabling.** IIS 6.0 helps protect server and other applications by automatically disabling Web sites and applications that fail too often within a short amount of time.

IIS 6.0 Manageability

Several important enhancements have been made in IIS 6.0 that provide new flexibility in how Web server infrastructure is managed, including:

- **XML-based configuration file.** Configuration data is stored as XML statements in a plain text file that can be edited using standard text editing tools and easily integrated with other system management tools.
- **Edit while running.** This feature enables manual or programmatic changes to the XML-based server configuration file while the server is running and without requiring a system reboot or recompilation.
- **Command-line administration and scripting.** Many common management tasks can be performed on single or multiple servers that are local or remote using a command-line interface. IIS 6.0 also has a complete scripting environment for automating common system administration tasks from the command line without having to use a graphical user interface.
- **Support for Windows Management Instrumentation (WMI).** WMI programming interfaces offer flexible ways to manage the Web infrastructure.

These features can reduce the amount of time it takes to manage larger server workloads and reduce staffing costs.

In addition, the IIS 6.management can be managed through the Windows System Resource Manager (WSRM). WSRM enables an administrator to set application resource consumption policies (for CPU and memory consumption, for example), to manage computer resources according to policies, to apply policies on a date/time schedule, and to generate, store, view, and export accounting records.

IIS 6.0 Security

Security is a critical aspect of server consolidation plans. With this release, IIS 6.0 reflects a focus on security. For example, in early 2002, the development work of all Windows engineers—more

than 8,500 people—was put on hold while the company conducted intensive security training. After the training was completed, the development teams analyzed the Windows code base, including IIS 6.0, to implement the new learning. This training represents a substantial investment to improve the security of the Windows platform. In addition, during the design phase of the product, Microsoft conducted extensive threat modeling to ensure that the company's software developers understood the type of attacks that the server might face in customer deployments.

There are several key security features important to consider when developing a server consolidation plan:

- **New server security defaults.** IIS 6.0 is not installed by default during installation or upgrade of Windows Server 2003, which reduces the Web infrastructure attack surface. When administrators choose to install IIS 6.0, it is configured to use maximum security settings by default.
- **Default low-privilege account.** All IIS 6.0 worker processes, by default, and all ASP built-in functions, at all times, run as Network Service user accounts. This new, built-in account has limited operating system privileges.
- **Constrained delegated authentication.** Domain administrators can limit the delegation of authorization credentials to a limited set of network resources.

For more information, see IIS 6.0 Security Changes in an earlier section.

Major Differences Among Versions of IIS

The following table lists significant differences across versions of IIS. The two key differences are:

- IIS 6.0 includes a kernel mode driver, HTTP.SYS, which receives the incoming requests to a Web server.
- IIS 6.0 includes two modes of operation: IIS 5.0 isolation mode and process isolation mode, which are discussed in the following sections.

IIS Version Differences

Area	IIS 4.0	IIS 5.0	IIS 5.1	IIS 6.0
Operating System	Windows NT 4.0	Window 2000	Windows XP Professional	Windows Server 2003 Family
Architecture	32 bit	32 bit	32 and 64 bit	32 and 64 bit
Application Process Model	TCP/IP Kernel Mtx.exe	TCP/IP Kernel Dllhost.exe (Multiple Dll hosts in medium or high isolation)	TCP/IP Kernel Dllhost.exe (Multiple Dll hosts in medium or high isolation)	HTTP.sys Kernel **IIS 5.0 isolation:** Intetinfo.exe in process or Dllhost.exe out of process **Worker process isolation:**

				W3wp.exe, multiple worker processes
Metabase Configuration	Binary	Binary	Binary	XML
Security	Windows Authentication SSL	Windows Authentication SSL Kerberos	Windows Authentication SSL Kerberos Security Wizard	Windows Authentication SSL Kerberos Passport support
Remote Administration	HTMLA	HTMLA	No HTMLA Terminal Services	Remote Administration tool (HTML) Web Server Appliance Kit (SAK) Terminal Services
Cluster Support	In Windows NT 4.0	IIS Clustering	Windows Support	Windows Support
WWW Services	IIS on NT 4.0	IIS on Windows 2000	IIS Optionally on Windows XP Professional	IIS on any Windows Server 2003 version

Isolation Modes

IIS 6.0 can run in one of two distinct application isolation modes: IIS 5.0 isolation mode and worker process isolation mode. Application isolation is the separation of applications by process boundaries that prevent the applications from affecting one another, and each IIS mode is configured differently.

Worker process isolation mode uses the redesigned architecture of IIS 6.0. This application isolation mode runs all application code in an isolated environment. However, unlike earlier versions of IIS, IIS 6.0 provides isolation without a performance penalty, because fewer processor instructions are run when switching from one application pool to another. Worker process isolation mode is compatible with most existing Web sites and applications. Whenever possible, run IIS 6.0 in worker process isolation mode to benefit from the enhanced performance and security in IIS 6.0.

IIS 5.0 isolation mode provides compatibility for applications that depend on the process behavior and memory model of IIS 5.0. Run IIS in this mode only when a Web site or application cannot run in worker process isolation mode, and run it only until the compatibility issues are resolved.

IIS 6.0 cannot run both application isolation modes simultaneously on the same server. In other words, a single server running IIS 6.0 cannot also run some Web applications in worker process

isolation mode and others in IIS 5.0 isolation mode. If applications require separate modes, the applications must run on separate servers.

Compatibility Issues

After you perform an upgrade of the operating system, IIS is configured to run in IIS 5.0 isolation mode by default. Before configuring IIS 6.0 to run in worker process isolation mode, you should evaluate whether your Web sites and applications are compatible with worker process isolation mode. Most of the compatibility issues with IIS 6.0 occur when configuring IIS 6.0 to run in worker process isolation mode.

One of the most common reasons for incompatibility with worker process isolation mode is that applications do not recognize custom ISAPI extensions or DLLs that depend on the memory and request processing models used by earlier versions of IIS. Determine application compatibility in your lab before upgrading your existing IIS server, and if you determine that your applications are not compatible with worker process isolation mode, you can run the applications in IIS 5.0 isolation mode.

Isolation Mode Matrix

Upgrade Path/Needs	IIS 5.0 Isolation Mode	Process Isolation Mode
Windows NT 4.0: Upgrade to Windows Server 2003	✔ [4]	
Windows NT 4.0: Clean install of Windows Server 2003		✔
Windows 2000: Upgrade to Windows Server 2003	✔ [5]	
Application with dependency on older memory model: Needs to run in-process with IIS or has dependency on System account	✔	
ASP.NET 1.0: Previously installed and dependent on 1.0 behavior not .NET Framework 1.1	✔	
Need for most secure model, application recycling abilities, and new features of IIS 6.0		✔

Enabling IIS 6.0 After an Upgrade

For security reasons, the WWW Publishing service is disabled when you upgrade from Windows 2000 Server or Windows 2000 Advanced Server to Windows Server 2003 or Windows Server 2003, Enterprise Edition, respectively. In a Windows 2000 Server installation, IIS 5.0 is installed by default, and in many cases the WWW service was not used. As a result, the WWW service is now disabled after an upgrade.

---

[4] IIS is not disabled by upgrade.

[5] IIS is disabled by default

To decrease the attack surface of a server, IIS 6.0 is disabled by default when you upgrade from Windows 2000 Server to Windows Server 2003 unless you do one of the following:

- For manual or unattended upgrades, run the **IIS Lockdown Tool** on your Windows 2000 Server before starting the upgrade process.
- For manual or unattended upgrades, add the registry entry **RetainW3SVCStatus** to the registry.
- For unattended upgrades, add the entry **DisableWebServiceOnUpgrade = False** in the unattended install script.
- Continue with the upgrade and enable the WWW service after upgrade.

Windows Server 2003 Processing Architecture

The processing architecture of IIS 6.0 varies depending on the configuration of the application isolation setting. When the setting is configured for IIS 5.0 isolation mode, calls coming into HTTP.sys are routed to a user mode process: Inetinfo.exe, Dllhost.exe, or Aspnet_wp.exe. Which process handles the call depends on the particular type of request as well as how the virtual directory is configured. All ASP.NET applications run under the Aspnet_wp.exe process. However, traditional ASP Web applications run as follows:

- Those with a low application protection setting run under Inetinfo.exe.
- Those with a medium application protection setting run under the shared instance of Dllhost.exe.
- Those with a high application protection setting run under their own instance of Dllhost.exe.

To control the process in which an ASP application runs, you can configure the Application Protection setting to low, medium, or high using the dialog box shown in Figure 52.

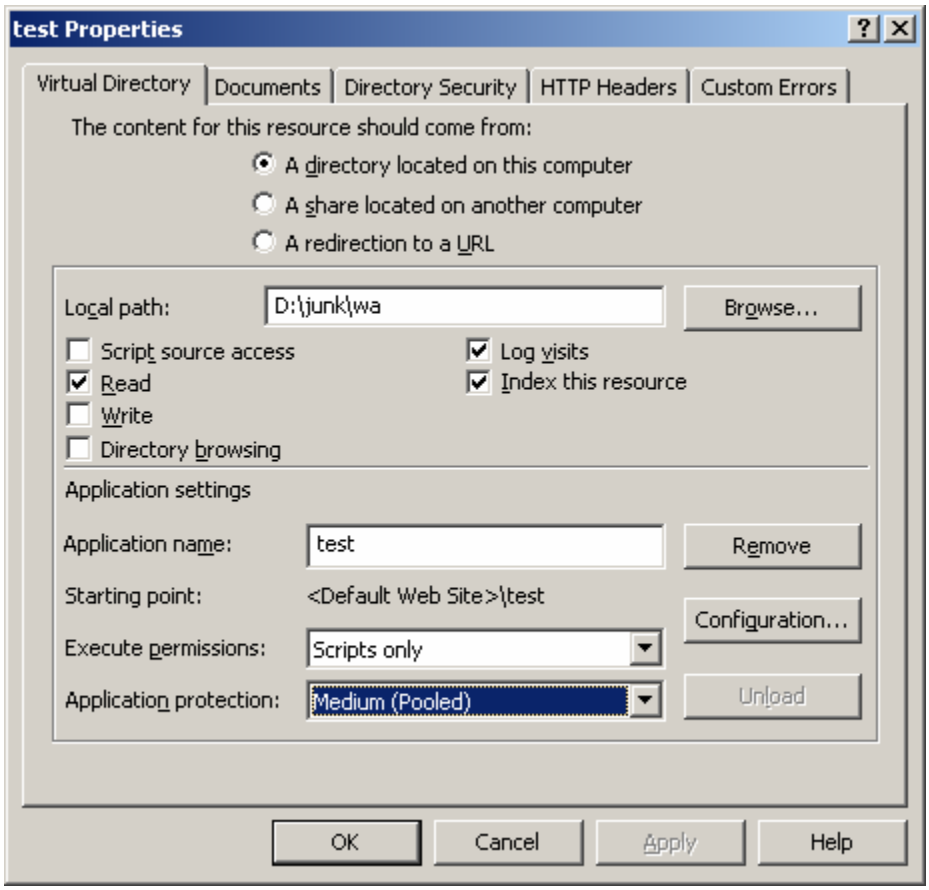


Figure 52. Application protection with IIS 5.0 isolation mode

By comparison, in worker process isolation mode, all requests for ASP.NET and ASP Web applications are handled by an instance of W3WP.exe. You can create more application pools and isolate virtual directories to run under a specific application pool.

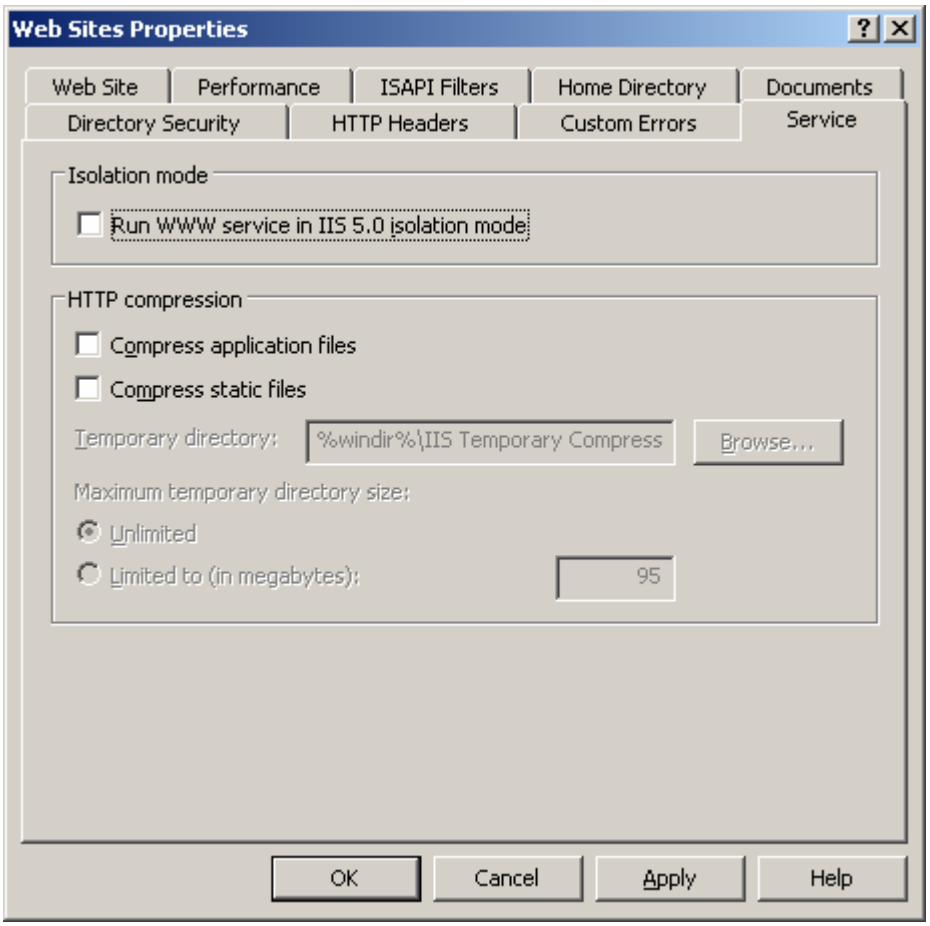
Note By default, when an instance of the W3WP.exe process starts, it runs under the identity of NetworkService, not LocalSystem or IWAM_*MachineName*.

Changing Application Isolation

Worker process isolation mode is the preferred mode and also the default mode for clean installations of Windows Server 2003. However, for upgrades of Windows NT Server 4.0, you must reconfigure the application isolation mode manually.

To change from isolation mode to worker process isolation mode:

1. Right-click **Web Sites** and click **Properties**.
2. Click the **Service** tab as shown:



3. Clear the **Run WWW service IIS 5.0 isolation mode** check box.

After changing the isolation mode, the server runs in worker process isolation mode.

For more information about enabling IIS 6.0 when you upgrade, download the Windows Server 2003 Deployment Kit: Deploying IIS 6.0 resources from the Microsoft Download Center.

Effects of Isolation Mode on the IIS MMC Snap-In

Several changes to the MMC snap-in for IIS occur after you change the application isolation mode to worker process isolation mode as the figures below show. Figure 53 shows IIS Explorer in IIS 5.0 isolation mode, and the Figure 54 shows it in worker process isolation mode, which includes the addition of an Application Pools folder:

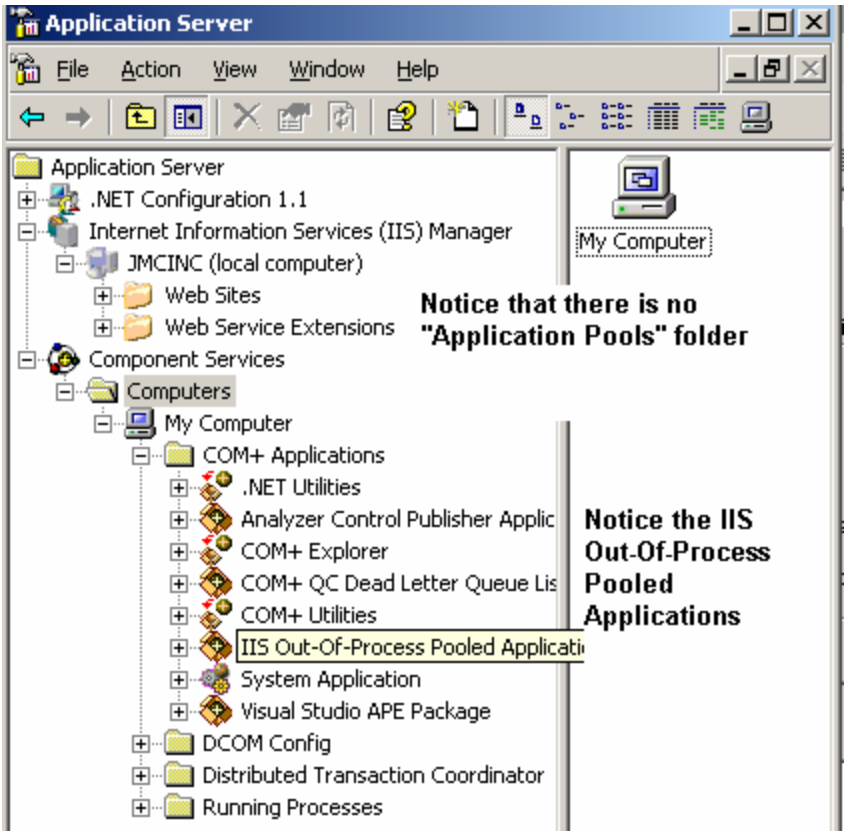


Figure 53. Out-of-process pooled applications in IIS 5.0 isolation mode

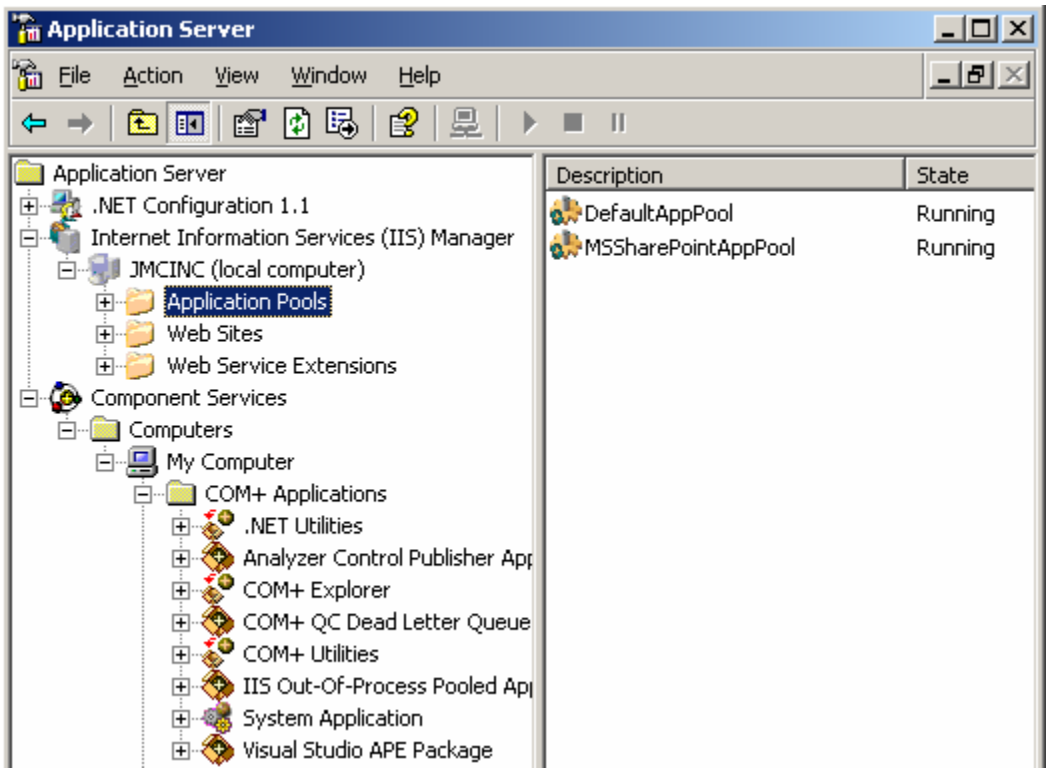


Figure 54. Application Pools folder in worker process isolation mode

Configuring Application Pools

When running in worker process isolation mode, a virtual directory can be configured to run under a specific application pool. To change a virtual directories application pool, you use the **Home Directory** tab of the **Web Site Properties** dialog box, as the following figure shows.

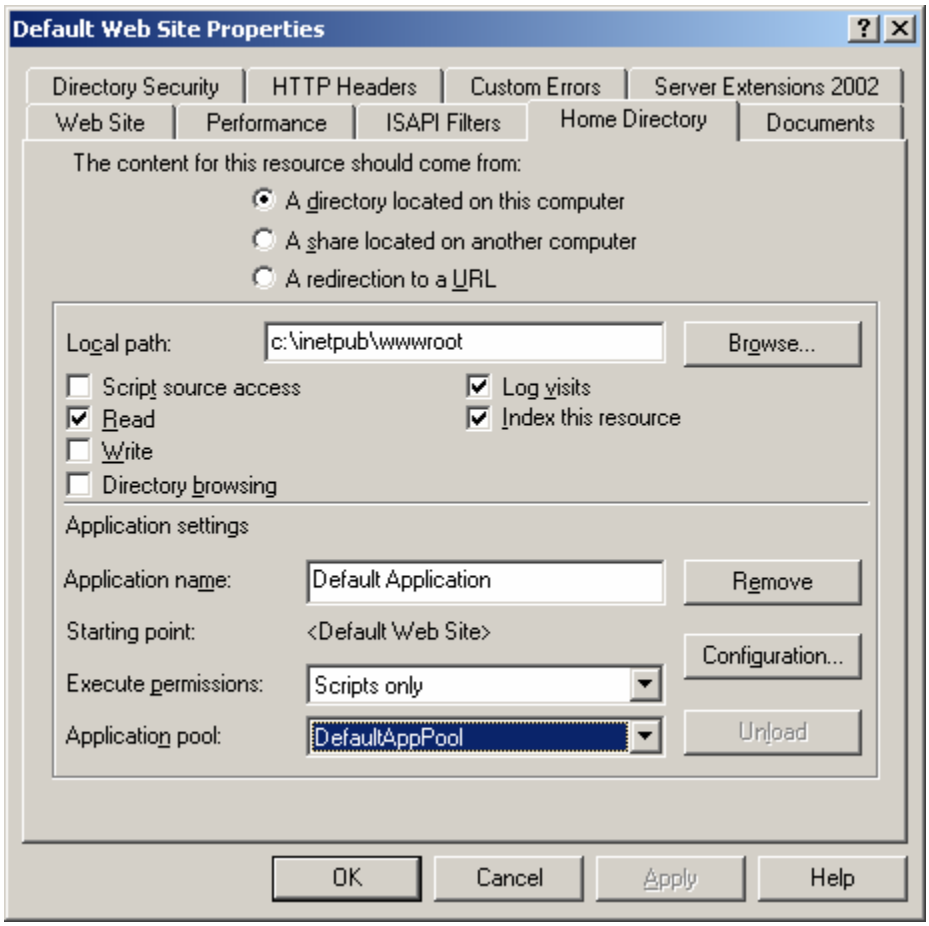


Figure 55. In worker process isolation mode, a virtual directory can be configured to run under a specific application pool in the Web Site Properties dialog box

Applications After Upgrade

Most applications run under the new worker process isolation mode without additional changes. However, the identity used by a process may need to be configured after you upgrade. If you configure an application pool to run as a custom identity, make sure to add the identity of the account to the new IIS_WPG group that is created when upgrading. IIS_WPG is a user group provided by IIS 6.0. IIS_WPG group membership provides the minimum set of user rights and permissions required to run an application. It provides a convenient way to use a specific user account that would be a member of IIS_WPG for the worker process identity account without having to manually assign the user rights and permissions to that account. In the cases where the account is not in the IIS_WPG group and does not have the appropriate permissions, the worker process will fail to start.

The following table lists some common configurations before the upgrade and possible configurations after the upgrade.

Application Upgrade Paths

Application	Process/Identity Before	Process/Identity After
Application A	In-Process/LocalSystem	Default Pool/Network Service
Application B	Isolated/IWAM_*MachineName*	Default Pool /Network Service
Application C	Isolated/Specific Identity	Default Pool /Network Service
Application D	Isolated/Specific Identity	Default Pool /Specific Identity
Application E	Isolated/IWAM_*MachineName*	Default Pool /Local System
Application F	Isolated/IWAM_*MachineName*	New Pool/Network Service
Application G	Isolated/IWAM_*MachineName*	New Pool/Specific Identity

ISAPI Extension Settings

If an upgrade is performed, ISAPI extensions are allowed; however, if a clean installation is performed, ISAPI extensions are prohibited. As the figure below shows, after upgrading from Windows NT Server 4.0, everything is allowed.

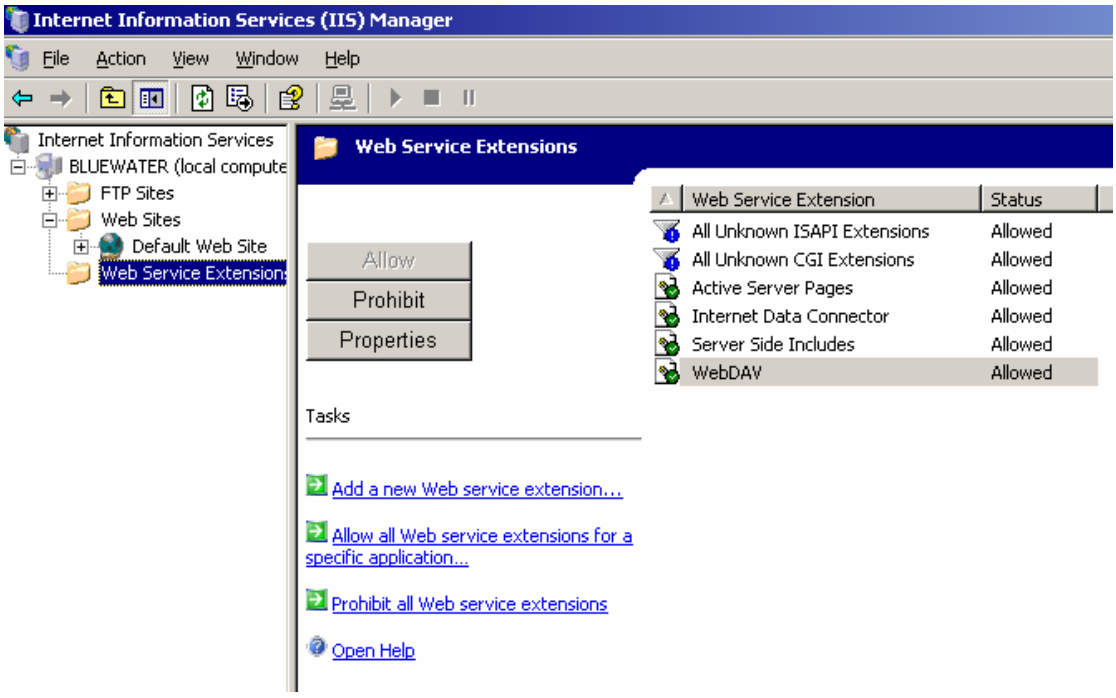


Figure 56. Allowed ISAPI extensions after an upgrade

If a clean installation is performed instead, and the Application role configured, everything is prohibited except ASP.NET as the following figure shows.

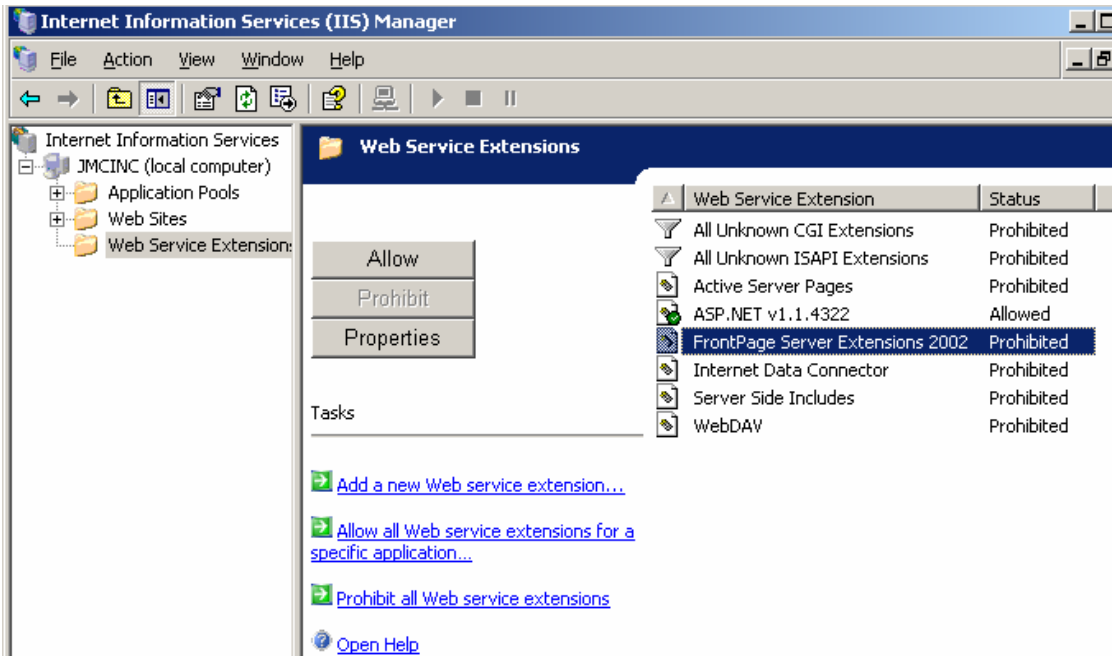


Figure 57. Prohibited IIS ISAPI extensions After a clean installation

ISAPI Filters Removed

The functionality for many of the ISAPI filters for earlier versions of IIS are now built into IIS. The following table highlights these changes.

ISAPI Filters Integrated into IIS 6.0

ISAPI Filter Function	ISAPI Filter File Name	Location
Compression	SSPIFILT.dll	Integrated into IIS 6.0
SSL Encryption	COMPFILT.dll	Integrated into IIS 6.0
Kerberos Authentication	MD5FILT.dll	Integrated into IIS 6.0

Upgrading ASP Web Applications

When upgrading ASP Web applications to Windows Server 2003, note the following:

- **Allow ASP extension.** Make sure the ASP extension is set to Allowed, the default setting when upgrading Windows NT Server 4.0 to Windows Server 2003. With a clean installation ASP will be prohibited, as noted earlier.
- **Enable server-side script.** ASP pages written with VBScript or ECMAScript (JScript, JavaScript) will not run until the ASP ISAPI extension is enabled.

Upgrading ASP Web Applications to ASP.NET Applications

Application written with VBScript must to be ported to Visual Basic .NET or C# because VBScript is no longer supported under ASP.NET. Migrating code to Visual Basic .NET is not as simple as renaming an ASP page from .ASP to .ASPX. An upgrade requires significant code changes.

Because all ASP.NET pages are compiled into assemblies, you gain from significant performance improvements. Pages are no longer interpreted every time they run. Applications now have complete support for the rich type system of the common language runtime and all the class libraries defined in the Framework Class Libraries.

For a complete discussion of the developer needs for upgrading, see Migrating ASP Pages to ASP.NET on the MSDN® Web site.

ASP.NET 1.0 Applications and ASP.NET 1.1 Applications

When upgrading an existing server on which are installed ASP.NET applications that use .NET Framework 1.0, the resulting upgraded computer is configured to use .NET Framework 1.1. Version 1.0 remains installed in what is called side-by-side deployment. However, side-by-side deployment is supported only when running in IIS 5.0 isolation mode. For more information, see Side-by-side Deployments of .NET Framework 1.0 and 1.1later in this guide.

Most ASP.NET 1.0 applications run fine under the new worker process isolation mode; however, some ASP.NET 1.0 Web applications do not run correctly with .NET Framework 1.1, primarily because of the tightened security settings. For example, under version 1.0, you could pass a SQL connection string with a user ID and a blank password and succeed. Under version 1.1, this action is not allowed.

You can configure individual applications to determine which version of the framework to run by configuring the script maps for each virtual directory. For more information, download the Windows Server 2003 Deployment Kit: Deploying IIS 6.0 resources. See the “Upgrading an IIS Server to IIS 6.0” chapter.

Exchange Server

More than just e-mail, Exchange has become a crucial system in most companies and the backbone of many communications infrastructures. In many organizations, the Exchange 5.5 messaging infrastructure performs adequately; however, the software running the messaging infrastructure is nearing the end of its product life cycle. Organizations looking to upgrade from Exchange Server 5.5 in a Windows NT 4.0 environment have been given an opportunity to upgrade with relative ease to both Windows Server 2003 and Exchange Server 2003. Microsoft is providing new and improved tools for both Windows upgrades and Exchange upgrades. These tools and the backward compatibility offered in these new products are designed to help ease the task of upgrading.

This section analyzes the feasibility of upgrading the current Exchange 5.5 e-mail infrastructure to Exchange 2003.

Note Exchange is an electronic mail *server* product, not to be confused with Microsoft Outlook®, an electronic mail *client*.

Exchange 2000 and Exchange 2003 Considerations

Exchange 2003 is intended as an incremental upgrade to Exchange 2000 with most of the focus on added features and not major architecture changes. The release of Exchange 2003 closely follows the release of Windows Server 2003. This means that by the end of 2003, there will be two upgrade paths for organizations using Exchange 5.5. Exchange 5.5 implementations can either be upgraded to Exchange 2000 or to Exchange 2003.

With the upcoming end to the Exchange 5.5 product life cycle, many organizations face the same question: Do we upgrade to Exchange 2000 or skip Exchange 2000 in favor of Exchange 2003? Many factors can play a role in a decision of this magnitude. Hardware availability and cost, availability of upgrade tools, feature improvements, and reliability are just a few of the other factors that need to be addressed.

Product Life Cycle Considerations

Exchange 2003 offers all the improvements of Exchange 2000 plus many added improvements and the benefit of a full five-year life cycle. Also, Exchange 2003 does not require any more hardware than Exchange 2000 so the decision to upgrade to Exchange 2003 should not cost any more than an upgrade to Exchange 2000. Exchange 2003 also offers a full array of deployment tools to help ease the upgrade process from either Exchange 5.5 or Exchange 2000. In contrast, the tools offered by Exchange 2000 are minimal and lack documentation.

An understanding of Microsoft product life spans can also be helpful in this decision-making process. Microsoft products typically have a five-year life span. After five years, an earlier version is no longer supported. This means that Microsoft Technical Support Services is only minimally available for end-of-life-cycle products, and service packs or hot-fixes are no longer developed for newly discovered software problems. As 2003 ends, Microsoft will provide minimal support for Exchange 5.5.

Exchange 2000 reaches the end of its life cycle at the end of 2005. Technology aside, by upgrading to Exchange 2000 at the end of 2003, only two years remain in the Exchange 2000 life cycle. Given the fact that Exchange 5.5 is nearing the end of its life cycle, companies still running Exchange 5.5 face a decision about the next version. A strong case can be made for Exchange 2003 based on this single factor. Keep in mind that if an organization decides to upgrade to Windows Server 2003, Exchange 2003 becomes the default choice, because neither Exchange 5.5 nor Exchange 2000 run on Windows Server 2003. When the next version of Exchange becomes available, time should be spent planning an upgrade. With adequate planning, most of the upgrade should have very little impact on the current users of the system.

Many of the improvements in Exchange 2003 change the way users of Outlook 2003 work. Outlook 2003 is the current preferred client for accessing an electronic mailbox in Exchange 2003. One of the goals of Exchange 2003 is to present users with a common look when connecting to e-mail either locally while in the office or from a remote location. Enhancements to remote access features in Exchange 2003 help improve user productivity, an important consideration given the increasing number of users working from home either after hours or as telecommuters.

By skipping Exchange 2000 in favor of Exchange 2003, an organization can use Exchange 5.5 to the end of its life cycle. It is unrealistic nowadays to keep up with the latest versions of all information technology software. Costs, user downtime, upgrade resources, and education are a few of the many considerations facing organizations, influencing them to bypass new versions of software in favor of currently stable systems. Eventually, business-driven features, time, and product life cycles become reason enough for organizations to upgrade to newer software releases. By waiting for Exchange 2003, organizations running Exchange 5.5 have allowed Exchange to mature and thus provide an even greater set of features and better reliability.

Stability and Cost Factors

Many organizations decided to stay on Exchange 5.5 because of its stability and the cost to upgrade to Exchange 2000. In many instances, businesses were unable to provide a compelling reason to upgrade to Exchange 2000 even with its better compatibility with Active Directory. Microsoft understands this issue and has spent a great deal of development time engineering tools to help companies upgrade to Exchange 2003 from both Exchange 5.5 and Exchange 2000. These tools help companies to engineer a smooth upgrade to Exchange 2003.

The META Group, a provider of information technology research, advisory services, and strategic consulting, recommends that “organizations with current migration plans scheduled for completion by YE03 upgrade to Exchange 2000. Those companies planning for a 2H03 migration, with completion due in 2004, should wait for Titanium, thereby avoiding a dual-hop migration.”

META Group states that an upgrade project undertaken in late 2003 should include an upgrade to Exchange 2003, skipping Exchange 2000. To take this one step further, organizations with no urgent need to upgrade to Exchange 2000 should just wait until Exchange 2003 is available for production. By waiting for Exchange 2003, companies still running Exchange 5.5 can use the time to plan for Exchange 2003 and to test the product in a lab environment. This planning should also allow plenty of time for administrator training. Such a plan encompasses all the ingredients of a successful upgrade.

E-mail Infrastructure

Organizations must update their messaging infrastructure to provide the reliability required of a mission-critical application. In the past, messaging meant e-mail and was regarded as just another way to communicate—much like telephones, faxes, forms, and written documents are vehicles for sharing information. Today, it is no longer enough to deliver e-mail messaging and the Internet to the client. Survival in today's e-business world requires organizations to analyze changes in the marketplace correctly and respond instantly. A powerful messaging system makes this possible.

Many organizations currently use Exchange 5.5 server primarily to send and receive mail. If companies are going to react with speed and intelligence to changing demands of the marketplace, these companies must bridge barriers of time, distance, and technology to provide every employee in the organization with real-time access to the information they need. Using Exchange Server 2003, organizations can take advantage of their messaging infrastructure to further increase employee productivity with value-added collaborative solutions. Exchange Server 2003 uses a wide range of emerging digital technologies to give the users real-time access to the information they need—no matter their location.

Exchange Server 2003 is engineered to make use of the power of Windows Server 2003 and delivers unified management of all messaging, collaboration, and network capabilities, and resources. The Exchange Server 2003 computing environment offers a low cost of ownership and also provides improved fault tolerance and scalability designed for large, enterprise environments. Deploying Exchange Server 2003 helps companies provide their employees with the latest technological advances in corporate messaging as well as improved backup and recovery.

Microsoft has been running beta versions of Exchange Server 2003 since September 2002 to thoroughly this product in a production environment. Its reliability has been tested by most Microsoft employees, who have been using Exchange Server 2003 since the beginning of 2003.

Scalability and Disaster Recovery

Many companies run Exchange servers with very large information stores. Stores of 50 GB and larger are not uncommon. Exchange 5.5 can handle large information stores, but disaster recovery of such a large store can be a challenge at best. These Exchange 5.5 servers may perform well today, but organizations need to consider whether they are equipped to handle a large, corrupted information store. Exchange Server 2003 enables an organization to break up that information store into smaller and more manageable stores that still reside on a single server.

For example, in the sample upgrade scenario described in an earlier section, HGF Properties faced this decision. Their server ran Exchange 5.5, Standard Edition, with a 16-GB information store limit, and the server currently had a 15.8-GB store. A company in a situation like this probably shouldn’t wait to upgrade until Exchange Server 2003 ships. The best path is an immediate upgrade to Exchange 2000 Enterprise Edition.

Exchange Server 2003 provides many reasons to upgrade, but none is more important than its superior scalability and disaster recovery mechanisms. Consider how much it costs to lose messaging functionality for one hour, one day, or even a couple of days. Employees dislike even a 15-minute messaging outage. The costs associated with a significant e-mail outage are probably

considerable. Exchange Server 2003 provides better backup tools and server consolidation features than previous versions. Used in combination with Windows Server 2003, Exchange 2003 supports the new Volume Shadow Copy service technology, a feature that enables administrators to mirror the disk on which the Exchange data store resides, performing quick backups with no downtime.

Current versions of Exchange provide no built-in support for restoring a single lost or corrupted mailbox. An administrator must either reload the entire server or rely on third-party products to complete this task. Exchange Server 2003 provides single mailbox restores as a built-in feature. This single feature can greatly reduce the disaster recovery process when a single mailbox is lost or corrupted.

Exchange 5.5 supports a single messaging database (Store) to store saved messages for all mailboxes. The database continues to function as the store grows, but becomes very difficult to work with in a disaster recovery situation. Exchange Server 2003 provides for multiple messaging stores, which enable a single, large store to be broken into several smaller more manageable stores. These smaller stores support better disaster recovery scenarios and help minimize the impact of a recovery on the organization as a whole, because mailboxes are distributed across multiple stores.

Deployment Tools

Exchange Server 2003 is designed to coexist with both Exchange 2000 and Exchange 5.5. Microsoft is providing an extensive suite of deployment tools for Exchange 2003. These tools make planning and executing an upgrade to Exchange Server 2003 easier than previous upgrades. The tools are particularly useful for organizations upgrading away from Exchange 5.x with or without Active Directory. They can be used to inspect the current Exchange environment and detect current configuration items that could impede the upgrade process.

The Exchange Server Deployment Tools consist of a series of tools and documentation that lead you through the following process:

- Planning the deployment.
- Preparing Active Directory by using ForestPrep and DomainPrep.
- Installing Active Directory Connector (ADC) and ADC tools.
- Installing Exchange.
- Completing deployment and moving mailboxes and public folders.

Using ADC

One of the toughest tasks in upgrading Exchange 5.5 to Exchange 2000 or Exchange 2003 is the setup of ADC. ADC provides necessary communication from the Exchange 5.5 directory service and directory database to the Active Directory database used by both Exchange 2000 and Exchange 2003. In earlier versions, ADC was easy to configure incorrectly, which caused upgrade issues.

An accurate setup of the ADC is crucial to a successful upgrade from Exchange 5.5. ADC provides a collection of wizards and tools that help set up connection agreements by scanning the current Active Directory and Exchange 5.5 Directory and organization, and then automatically creating the recommended connection agreements. This tool is a tremendous asset to the Exchange 5.5 administrator undertaking an upgrade to Exchange 2003.

Upgrade Documentation

The documentation provided with the deployment tools package has been improved as well. Earlier editions of Exchange (including Exchange 2000) provided very few upgrade tools, and the documentation for the tools that did exist sometimes lacked detail. Microsoft has committed to making upgrades from Exchange 5.5 to Exchange 2003 as simple and robust as possible—another reason to consider upgrading directly to Exchange 2003 rather than Exchange 2000.

Feature Improvements in Exchange 2003

The following table summarizes the top feature enhancements in Exchange Server 2003.

New and Improved Features in Exchange Server 2003

Option	Description
Outlook Web Access (OWA)	The latest OWA interface looks more like the new Microsoft Office Outlook 2003 client and so provides users with a consistent experience whether in the office or on the road. Security and performance are improved as well, and spell checking, task scheduling, and anti-spam features have been added.
Outlook 2003	Outlook 2003 is optimized for use with Exchange 2003. A new interface streamlines access to personal folders and displays currently open e-mail messages. Using Exchange 2003 and Outlook 2003 in combination enhances the performance of the Outlook client over low bandwidth and unreliable WAN links so that remote Outlook users have a similar experience to users on a LAN. This benefit enables remote users in small offices to use a remote Exchange server rather than requiring a local Exchange server for performance reasons.
Mobile Access and Synchronization	Exchange 2003 offers support and communications for an expanded set of mobile devices. Support for iMode, cHTML, and WAP 2.0 micro-browsers enable users to access their e-mail using the latest handheld technology, such as personal display appliances (PDAs) and cell phones. Support is also provided for Short Message Service (SMS) that can alert always-on mobile devices when a new message arrives in the inbox. User can then synchronize the messages, if necessary.
Server consolidation	Exchange 2003 builds on the server consolidation features of Exchange 2000 and improves the use of server and storage resources by supporting the following: § Windows Server 2003 services that support Volume Shadow Copy service. Volume Shadow Copy service enables online backup of Exchange Storage Groups, so there's no need to take systems offline. § Instantaneous backup and restore, which removes one of the practical limits to the number of users supported on a single server—the time it takes to back up the mail storage. § Faster and more reliable synchronization. The client-to-server communication protocol has been rewritten and optimized. These efficiency gains help to

	deliver faster and consistent client performance without the expense of equipping remote offices with additional servers to run Exchange. § Outlook 2003 cache mode. Because Outlook 2003 operates primarily on its own cached copy of a user's mailbox, fewer requests are made to the server, reducing the server load per user and enabling more users to be supported per server.
Security	A number of important improvements have been made to increase the security of the Exchange system across several different fronts. Like Windows Server 2003, the default settings of Exchange Server 2003 for all system variables are selected to maximize system security. § OWA now uses cookie authentication and connection time-out processes to help eliminate the likelihood of security breaches through unattended browsers. Additionally, OWA supports the use of the S/MIME security protocol to send e-mail messages. § VSAPI, the virus-scanning API, has been improved to give administrators more deployment options. New junk e-mail message management capabilities help prevent unsolicited messages with support for connection filtering based on real-time blacklists, inbound recipient filtering, and beacon-blocking. In addition, VSAPI antivirus software can now run on Exchange gateway and bridgehead servers as well as mail servers. § Support for Internet Protocol security (IPSec) for managing front-end and back-end servers. § By adding Windows Server 2003, remote procedure calls (RPC) over HTTPS tunneling securely connect Outlook 2003 clients with Exchange Server 2003 without the need for a VPN.

Upgrading to Exchange Server 2000

Although many arguments favor an upgrade path that leads from Exchange 5.5 directly to Exchange 2003, an organization may want to consider upgrading to Exchange 2000 first.

One reason is that current Exchange 5.5 servers cannot be upgraded using the in-place upgrade method, whereby an existing server is upgraded directly to Exchange 2003. Only Exchange 2000 servers can be upgraded directly to Exchange 2003. However, in-place upgrades of Exchange servers can be problematic. Even a small corruption in the Exchange stores (databases) can disrupt the upgrade process. When very large Exchange stores are involved, the chance of failure increases. For organizations with large information stores in particular, an in-place upgrade would probably prove risky.

A less risky upgrade path involves the movement of mailboxes from one version of Exchange to another version of Exchange. Although more time-consuming than an in-place upgrade, this method tends to less invasive and so less risky.

Operating System Versions

Another consideration for organizations is the underlying operating system. Exchange Server 2003 runs on either Windows 2000 with SP3 or Windows Server 2003. However, to take maximum advantage of its features, Windows Server 2003 is required. For example, the new

backup strategy in Exchange Server 2003 is much more flexible when using the Volume Shadow Copy service that only Windows Server 2003 includes. Also, for those organizations that choose to upgrade to Windows Server 2003, the only choice for e-mail is Exchange Server 2003. For any organization needing greater operating system flexibility, an upgrade to Exchange Server 2000 may be preferred.

Risk Management

One of the main goals of any upgrade is risk management. To reduce the risks of the upgrade, the risks must be identified. Does Exchange Server 2003 pose any more risks than Exchange 2000? The short answer is yes, because of the relatively short time that Exchange Server 2003 has been in enterprise production. For this reason, organizations may prefer to upgrade to Exchange Server 2000 first.

Features Made Obsolete by Upgrading

Several features that existed in Exchange 2000 or Exchange 5.5 have been discontinued in Exchange 2003 or moved to other product lines. The following features are no longer in Exchange Server 2003:

- **Real-time collaboration features.** Exchange 2000 supports numerous real-time collaboration features such as chat, Instant Messaging, conferencing (using Exchange Conferencing Server), and multimedia messaging (also known as unified messaging). These features have been removed from Exchange Server 2003. Microsoft Office Real-Time Communications Server 2003 (RTC Server), previously code-named "Greenwich," is the new enterprise instant messaging (IM) solution and extensible real-time communications platform from Microsoft, currently under development. For more information, see the RTC Server home page on the Microsoft Office Web site at http://www.microsoft.com/office/preview/rtcserver/default.asp.
- **M: drive.** In earlier versions, the Exchange information store (which uses the \\.\BackOfficeStorage\ namespace) is mapped to the M: drive on an Exchange server. The M: drive mapping provides file system access to the Exchange store. However, in some cases, the mailbox store can become corrupted from file system operations, such as running a file-level virus scanner on the M: drive, or by running file backup software on the drive. As a result, the M: drive is disabled by default in Exchange Server 2003.
- **Key Management Service (KMS).** Exchange 2000 and Exchange 5.5 include KMS, which works with Windows 2000 certificate services to create a PKI for performing messaging. With a PKI infrastructure in place, users can send signed and encrypted messages to each other. KMS in Exchange 2000 provides a mechanism for enrolling users in advanced security and handles key archival and recovery functions. Exchange Server 2003 no longer includes KMS. The PKI included with Windows Server 2003 now handles the key archival and recovery tasks that were performed by KMS in Exchange 2000.

Upgrade Paths for Exchange Server 2003

When Exchange 2003 is released, you will be able to upgrade from Exchange 5.5 in one of two ways:

- Upgrade to Exchange 2000, and then upgrade to Exchange Server 2003. This option is best for organizations with a strong need to move away from Exchange 5.5.
- Upgrade directly to Exchange Server 2003. This option is recommended for other organizations.

Unless there is an immediate need to upgrade to Exchange 2000, it is probably best to wait for Exchange Server 2003. The tools and documentation have improved, and this version provides critical new features, such as spam defenses. Moreover, the extra risk associated with upgrading to a new release can be reduced by carefully introducing Exchange Server 2003. Exchange Server 2003 can be installed using a pilot program for testing purposes. The new server can be placed into production in minimal capacity to see how it responds to a production environment. Users can be slowly upgraded to the server as confidence in the server builds.

COM+ 1.5

Component services continue to be a fundamental application platform for many applications and developers. COM+ 1.5 is included in Windows Server 2003 and introduces many new features. This section provides a quick overview of key new features in COM+ 1.5 to be aware of when upgrading from Windows NT Server 4.0.

COM+ can be used to develop enterprise-wide, mission-critical, distributed applications based on the Windows platform. COM+ builds on and extends applications written using COM, MTS, and other COM-based technologies. COM+ handles many of the resource management tasks that developers previously had to program, such as thread allocation and security.

The new COM+ 1.5 features are not available in earlier platforms, such as Windows 2000, which supports COM+ 1.0. However, COM+ 1.5 applications are still serviced by the Dllhost.exe process for out-of-process applications (also known as server applications) and are contained in the caller's process for in-process applications (also know as library applications).

Feature Changes from Previous Releases

The Component Services administrative tool includes the following new features:

- **COM+ application security.** You can now configure the software restriction policy for your COM+ applications either by using the Component Services administrative tool or programmatically. The software restriction policy was created to help protect systems from unknown and possibly dangerous code and provides a mechanism where only trusted code is given unrestricted access to a user's privileges.
- **COM+ Queued Components.** In COM+ 1.0, you set the maximum number of threads for COM+ Queued Components messages by using a registry key. This setting was applied computer-wide, and each application used the same setting. However, now you can set a different maximum number of threads for each application.
- **Registry key change.** COM+ no longer reads the registry key HKLM\Software\Microsoft\COM3\Debug\QCListenerMaxThread.

New Features in COM+

Feature	Description
Application pooling	The new COM+ application pooling service adds scalability for single-threaded processes and integrates with the new COM+ application recycling service.
Application recycling	Application performance can degrade over time because of application problems such as memory leaks, non-scalable resource usage, and process failures. The COM+ application recycling service enables you to shut down an application automatically and restart it, thus reinitializing a failing process and reallocating memory it uses.
COM+ partitions	COM+ 1.5 introduces support for partitions, a feature that allows multiple configurations of COM+ applications to run simultaneously on the same computer. This feature can save you the cost and time-consuming effort of using multiple servers to manage different configurations of an application. For example, you can create a test and a development configuration of a COM+ application.

COM+ SOAP Service	The new COM+ SOAP service allows clients to access configured COM components on a network server by using XML and SOAP. The COM+ SOAP service enables you to easily deploy your COM+ applications across a network as XML Web services while maintaining centralized control.
Low-memory activation gates	With this release, Component Services automatically check memory before creating a COM+ server object. If the percentage of virtual memory available to the application falls below a fixed threshold, the activation fails before the object is created. By failing these activations that would normally run, the low-memory activation gates feature greatly enhances system reliability.
Pausing and disabling applications	Compared to earlier versions, COM+ applications are now more manageable. An administrator can pause and resume COM+ server applications or disable and enable COM+ library or server applications, or even individual configured components. Both the pausing and disabling features prevent future activations without affecting existing component instances.
Process dumping	COM+ now provides a solution to the problems associated with troubleshooting applications in a production environment. The new process dump feature enables a system administrator to dump the entire state of a process without terminating it. In this way, you can gather information about a problem without disturbing the running processes.

For more information about COM+, see What's New in COM+ 1.5 in the COM+ Software Development Kit Documentation on the MSDN Web site.

Side-by-side Deployments of .NET Framework 1.0 and 1.1

A key benefit of .NET Framework 1.1 in Windows Server 2003 is that different versions can be installed side-by-side on a single computer. For example, version 1.0 and version 1.1 of the .NET Framework can be installed on the same computer, enabling you to better support a variety of application configuration scenarios. Support for side-by-side deployment benefits administrators and developers alike by eliminating the hassles associated with maintaining the DLLs of old.

In the context of this guide, versions are defined as follows:

- A 1.0 application is an application built with and intended for .NET Framework 1.0. All Visual Studio .NET 2002 applications are built this way.
- A 1.1 application is an application built with and intended for .NET Framework 1.1. All Visual Studio .NET 2003 applications are built this way.

All versions of Windows Server 2003 ship with .NET Framework 1.1.

How Side-by-Side Versions Work

Side-by-side versions of the .NET Framework are supported in much the way that the Visual Basic runtime works. With Visual Basic, a developer can build an application that targets the Visual Basic 5.0 runtime and deploy it to a computer. Later, an application can be built that targets the Visual Basic 6.0 runtime and deployed to the same computer. In the end, both versions 5.0 and 6.0 of the Visual Basic runtime are installed on the computer. However, an application targeted for a particular version works only with the version they are compiled against—behavior that differs from the runtime and the .NET Framework.

With the .NET Framework, an application can be built and compiled against version 1.0, and then even if version 1.1 is installed on a computer, an administrator can redirect the application to use version 1.1 of the runtime. A developer is not required to recompile the original application against version 1.1. In a side-by-side installation of the .NET Framework, an application is redirected dynamically to a newer version of the runtime and .NET Framework libraries without any intervention from the developer.

Assemblies and Side-by-Side Execution

Side-by-side execution is the ability to store and run multiple versions of an application or component on the same computer. This means that you can have multiple versions of the runtime, and multiple versions of applications and components that use a version of the runtime, on the same computer at the same time. Side-by-side execution gives you more control over the versions of a component an application binds to and more control over the version of the runtime an application uses.

Support for side-by-side storage and execution of different versions of the same assembly is an integral part of strong naming and is built into the infrastructure of the runtime. Because the strong-named assembly's version number is part of its identity, the runtime can store multiple versions of the same assembly in the global assembly cache and load those assemblies at run time.

Although the runtime provides you with the ability to create side-by-side applications, side-by-side execution is not automatic. For more information, see Side-by-Side Execution on the MSDN Web site and the .NET Framework Software Development Kit Help.

Changes that Affect Backward or Forward Compatibility

A strong effort has been made to ensure that applications compiled against version 1.0 of the framework can run against version 1.1. Applications compiled against version 1.1 may also work against 1.0 in some cases, but the primary concern has been to support compatibility from 1.0 to 1.1.

With any new version, some changes may cause an application to behave differently or break. Some of the main concerns are as follows:

- **Change in trust attributes.** In version 1.0 and 1.1, applications that receive less than full trust from the runtime code access security system cannot call shared managed libraries unless the library writer specifically allows them to through the use of the *AllowPartiallyTrustedCallersAttribute* attribute. If you plan on using libraries from partially trusted code, you need to be aware that some libraries will not be available to your code. In version 1.1, System.Web.dll, System.Web.Mobile.dll, and System.Web.RegularExpressions.dll are included in the list of assemblies that have the *AllowPartiallyTrustedCallersAttribute* and can be called from partially trusted code.
- **Change in default security policy.** Default security policy has been changed so that applications executing from the Internet zone and assigned to the Internet zone code group now receive permissions associated with the Internet permission set. As a result, applications from the Internet now receive sufficient permission to execute. In the .NET Framework 1.0 Service Pack 1 (SP1) and Service Pack 2 (SP2), such applications received the permissions associated with the Nothing permission set and could not execute.

For more information about these changes, refer to the Help included with the .NET Framework Software Development Kit.

For a detailed list of all the changes that may affect backward and forward compatibility, see Backwards Breaking Changes from Version 1.0 to 1.1 on the Got Dot Net Web site, the .NET Framework community site, at http://www.gotdotnet.com/team/changeinfo/Backwards1.0to1.1/default.aspx.

Side-by-Side Execution Examples

The following illustration shows several applications using two different versions of the runtime on the same computer. Applications A, B, and C use runtime version 1.0, while application D uses runtime version 1.1.

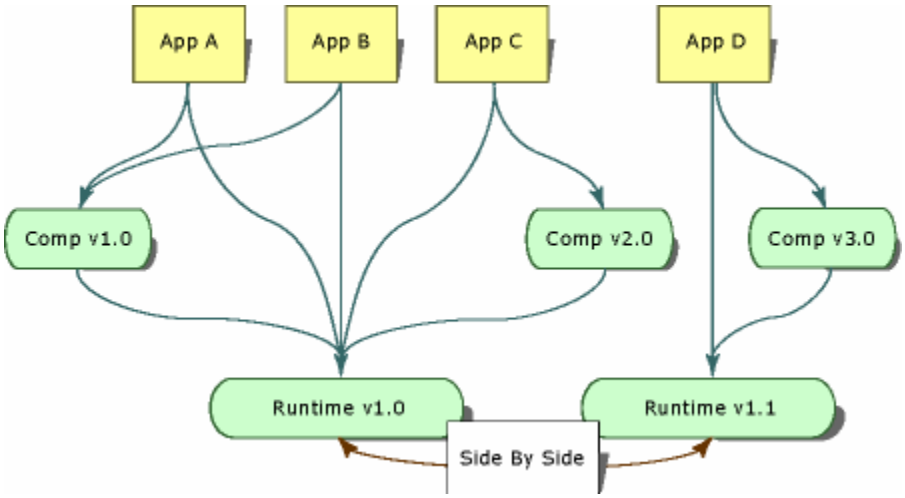


Figure 58. Side-by-side execution of two versions of the runtime

The .NET Framework consists of the common language runtime and about two dozen assemblies that contain the API types. The runtime and the .NET Framework assemblies are versioned separately. For example, version 1.0 of the runtime is actually version 1.0.3705.0, while version 1.0 of the .NET Framework assemblies is version 1.0.3300.0.

The following illustration shows several applications using two different versions of a component on the same computer. Application A and B use version 1.0 of the component while Application C uses version 2.0 of the same component.

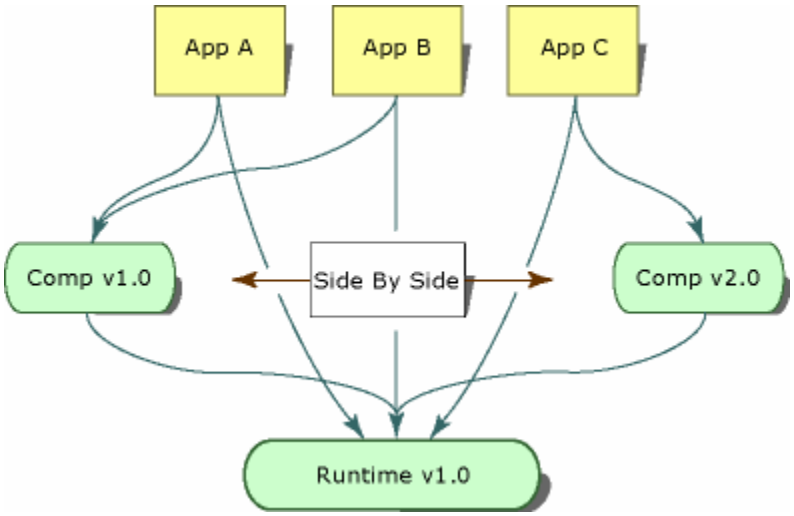


Figure 59. Side-by-side execution of two versions of a component

Benefits of Side-by-Side Execution

Prior to Windows XP and the .NET Framework, DLL conflicts occurred because applications were unable to distinguish between incompatible versions of the same code. Type information contained in a DLL was bound only to a file name. An application had no way of knowing if the

types contained in a DLL were the same types that the application was built with. As a result, a new version of a component could overwrite an older version and break applications.

Side-by-side execution and the .NET Framework provide the following features to eliminate DLL conflicts:

- **Strong-named assemblies.** Side-by-side execution uses strong-named assemblies to bind type information to a specific version of an assembly. This functionality prevents an application or component from binding to a version of an assembly that is not valid. Strong-named assemblies also allow multiple versions of a file to exist on the same computer and to be used by applications.
- **Version-aware code storage.** The .NET Framework provides version-aware code storage in the global assembly cache, a computer-wide code cache present on all computers on which the .NET Framework is installed. The global assembly cache stores assemblies based on version, culture, and publisher information, and supports multiple versions of components and applications.
- **Isolation.** Using the .NET Framework, you can create applications and components that execute in isolation, an essential component of side-by-side execution. Isolation involves being aware of the resources you are using and taking care when sharing resources among multiple versions of an application or component. Isolation also includes storing files in a version-specific way. For more information about isolation, see “Guidelines for Creating Applications and Components for Side-by-Side Execution” in the .NET Framework Software Development Kit Help.

Appendix A: Sample Active Directory Upgrade

This appendix continues the sample upgrade scenario provided earlier in this document (see Sample In-Place Upgrade for a Windows NT PDC earlier in this guide). The steps below explain how to finish the upgrade by upgrading the Windows NT 4.0 domain to an Active Directory domain. This process is the first action item after the upgrade of a Windows NT 4.0 domain controller is complete.

The Active Directory Installation Wizard simplifies the tasks associated with upgrading a Windows NT domain to Windows Server 2003 Active Directory. Active Directory Installation Wizard installs and configures domain controllers, which provide network users and computers access to the Active Directory service. Any member server (except those with restrictive license agreements) can be promoted to domain controllers using the Active Directory Installation Wizard.

There is more than one way to start the wizard, but the preferred method is to type **DCPROMO** on the **Run** command line. However, the Active Directory Installation Wizard also automatically starts after upgrading a Windows NT 4.0 domain controller.

The figure below shows the wizard that automatically starts after the upgrade of a PDC.

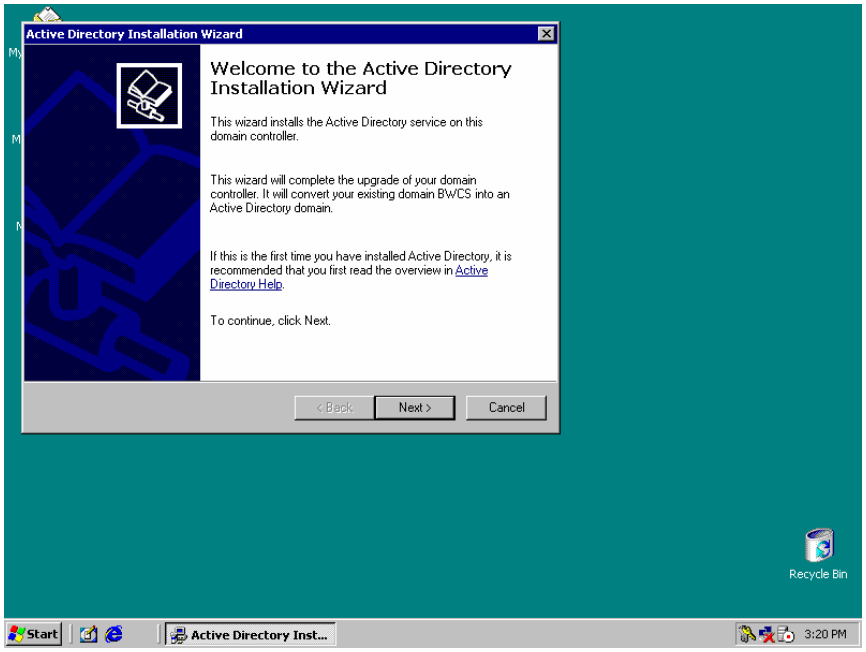

Active Directory Installation Wizard
Welcome to the Active Directory Installation Wizard
This wizard installs the Active Directory service on this domain controller.
This wizard will complete the upgrade of your domain controller. It will convert your existing domain BWCS into an Active Directory domain.
If this is the first time you have installed Active Directory, it is recommended that you first read the overview in Active Directory Help.
To continue, click Next.
< Back
Next >
Cancel
Recycle Bin
Start
Active Directory Inst...
3:20 PM

Figure 60. Active Directory Installation Wizard opening screen

Next, warning message appears about down level client accessibility appears:

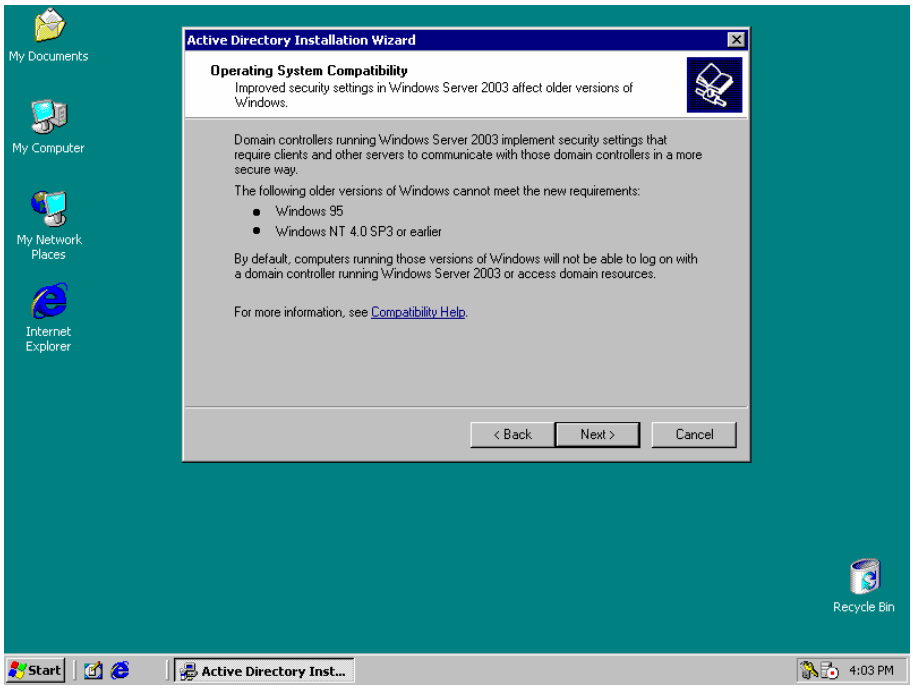

My Documents
My Computer
My Network Places
Internet Explorer
Active Directory Installation Wizard
Operating System Compatibility
Improved security settings in Windows Server 2003 affect older versions of Windows.
Domain controllers running Windows Server 2003 implement security settings that require clients and other servers to communicate with those domain controllers in a more secure way.
The following older versions of Windows cannot meet the new requirements:
Windows 95
Windows NT 4.0 SP3 or earlier
By default, computers running those versions of Windows will not be able to log on with a domain controller running Windows Server 2003 or access domain resources.
For more information, see Compatibility Help.
< Back
Next >
Cancel
Recycle Bin
Start
Active Directory Inst...
4:03 PM

Figure 61. Operating system compatibility warning

The next dialog box asks whether to create a domain in a new forest, create a child domain in an existing domain tree, or create a domain tree in an existing forest. In this example the computer is a Windows NT 4.0 PDC, so it is assumed there is no existing forest, and the option is chosen to create a domain in a new forest.

Next, a name for the domain must be typed. Figure 62 shows the screen that appears when a DNS name is necessary.

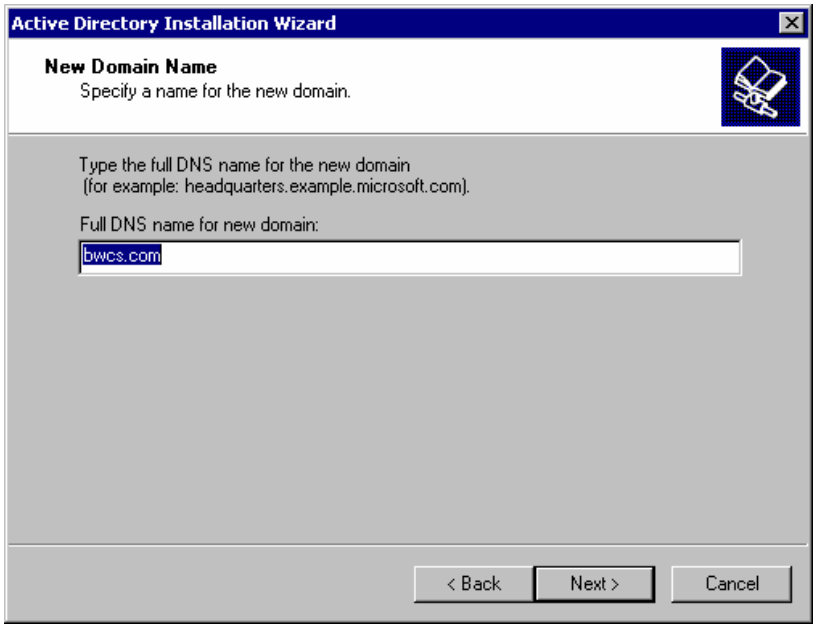

Active Directory Installation Wizard
New Domain Name
Specify a name for the new domain.
Type the full DNS name for the new domain
(for example: headquarters.example.microsoft.com).
Full DNS name for new domain:
bwcs.com
< Back
Next >
Cancel

Figure 62. Specify a name for the domain

Note All Windows NT administrators should have an excellent understanding of DNS, which is critical to the performance of Active Directory. Even something as simple as joining a workstation to a domain requires DNS to be working properly.

After typing the name of the domain, a dialog box prompts the administrator for the forest functional level as the following figure shows.

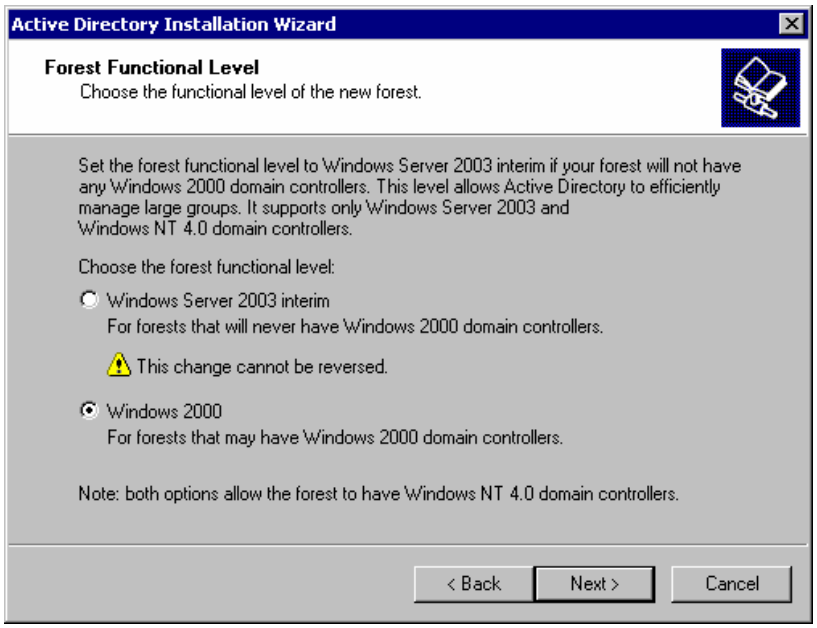

Active Directory Installation Wizard
Forest Functional Level
Choose the functional level of the new forest.
Set the forest functional level to Windows Server 2003 interim if your forest will not have any Windows 2000 domain controllers. This level allows Active Directory to efficiently manage large groups. It supports only Windows Server 2003 and Windows NT 4.0 domain controllers.
Choose the forest functional level:
Windows Server 2003 interim
For forests that will never have Windows 2000 domain controllers.
This change cannot be reversed.
Windows 2000
For forests that may have Windows 2000 domain controllers.
Note: both options allow the forest to have Windows NT 4.0 domain controllers.
< Back
Next >
Cancel

Figure 63. Select the forest functional level

The forest functional level provides for backward compatibility with Windows 2000 domain controllers. If no Windows 2000 servers will provide domain controller services such as authentication, the Windows Server 2003 interim option can be selected. Keep in mind that there is no going back after this option is selected. Compatibility with Windows NT 4.0 domain controllers is available in both modes. There are four domain functional levels in Windows Server 2003:

- **Windows 2000 Mixed.** Supports Windows NT 4.0, Windows 2000, Windows Server 2003.
- **Windows 2000 Native.** Supports Windows 2000, Windows Server 2003.
- **Windows Server 2003 Interim.** Supports Windows NT 4.0, Windows Server 2003.
- **Windows Server 2003.** Supports Windows Server 2003.

By choosing the default option of Windows Server 2003 Interim, Windows Server 2003 will allow for backward compatibility Windows NT 4.0 domain controllers. When in doubt, choose this option. A change to support only Windows Server 2003 can be made at any time through a dialog box in Active Directory Users and Computers. After making this important choice the installer is presented with a dialog box to choose the location to store the Active Directory database as is shown in the following figure.

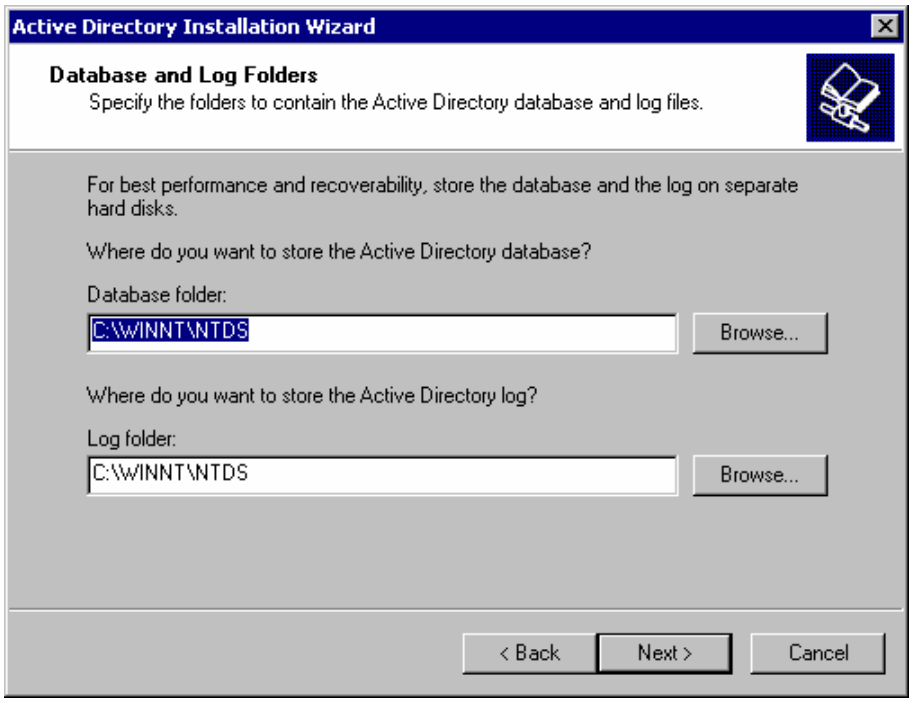

Active Directory Installation Wizard
Database and Log Folders
Specify the folders to contain the Active Directory database and log files.
For best performance and recoverability, store the database and the log on separate hard disks.
Where do you want to store the Active Directory database?
Database folder:
C:\WINNT\NTDS
Browse...
Where do you want to store the Active Directory log?
Log folder:
C:\WINNT\NTDS
Browse...
< Back
Next >
Cancel

Figure 64. Choose location of Active Directory database

On an upgraded Windows NT 4.0 domain controller it may be prudent to store the Active Directory database on a separate partition than the operating system due to the possible lack of disk space on a 4-GB partition. Next, the Sysvol folder must be setup in the proper location as the following figure shows.

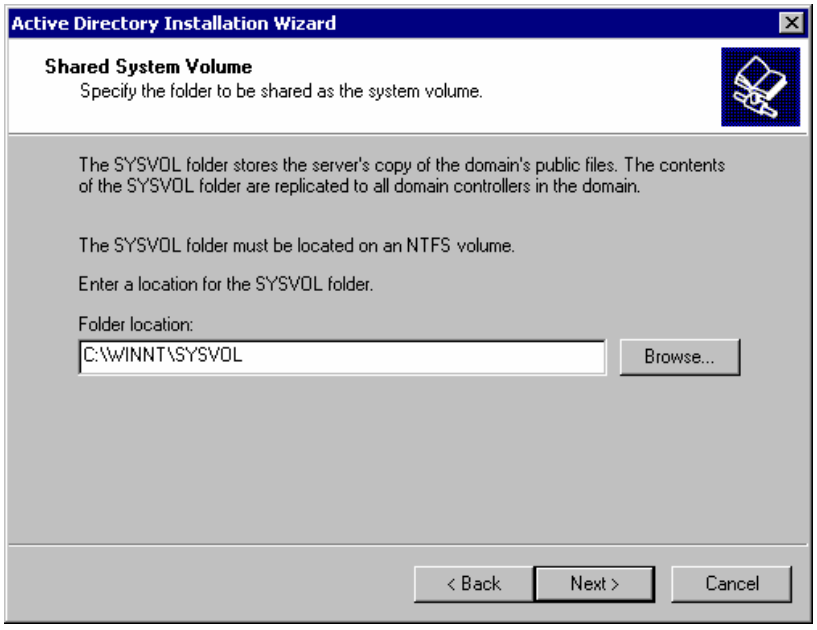

Active Directory Installation Wizard
Shared System Volume
Specify the folder to be shared as the system volume.
The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.
The SYSVOL folder must be located on an NTFS volume.
Enter a location for the SYSVOL folder.
Folder location:
C:\WINNT\SYSVOL
Browse...
< Back
Next >
Cancel

Figure 65. Specify location of shared Sysvol folder

Next, Windows Server 2003 indicates that it needs to communicate with DNS to set up the records needed for Active Directory to function properly. This Windows NT 4.0 domain controller may be the first Windows Server 2003 server in the domain, so there is a good chance that no DNS servers exist at this stage of the upgrade. The figure below shows the diagnostic results that state the problem.

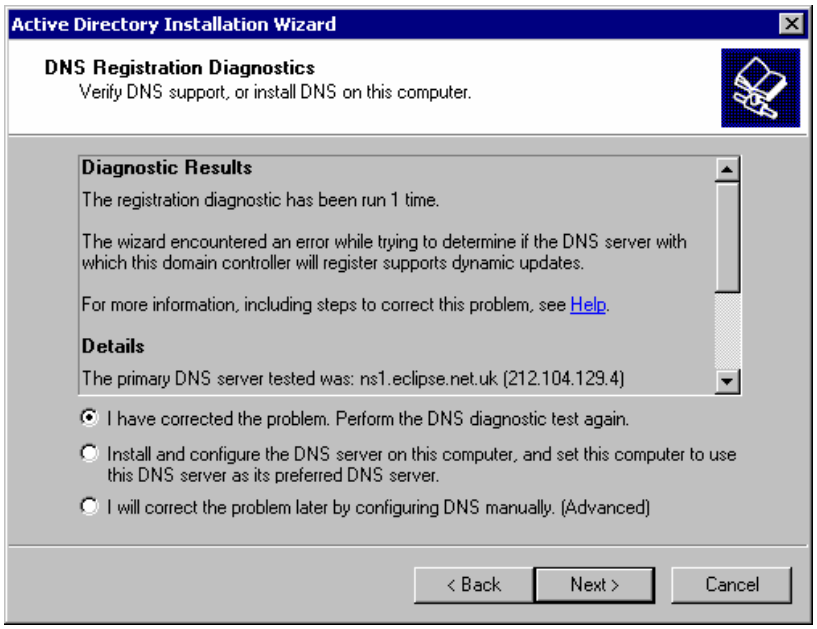

Active Directory Installation Wizard
DNS Registration Diagnostics
Verify DNS support, or install DNS on this computer.
Diagnostic Results
The registration diagnostic has been run 1 time.
The wizard encountered an error while trying to determine if the DNS server with which this domain controller will register supports dynamic updates.
For more information, including steps to correct this problem, see Help.
Details
The primary DNS server tested was: ns1.eclipse.net.uk (212.104.129.4)
I have corrected the problem. Perform the DNS diagnostic test again.
Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server.
I will correct the problem later by configuring DNS manually. (Advanced)
< Back
Next >
Cancel

Figure 66. DNS Warning dialog box

In this example, this computer is the first to be upgraded to Windows Server 2003. There are no other DNS servers available in the domain. The option to **Install and configure the DNS server on this computer** was chosen. This option also makes sure the TCP/IP settings are changed to point to itself as the primary DNS server. Although not necessary, it is a good idea to allow a DNS server to create and handle all the necessary Active Directory records.

In order for Active Directory to start up and function properly after the upgrade, a DNS server must be present. The DNS server used must support SRV records and dynamic updates among other things to allow Active Directory to work properly. Careful inspection of DNS should follow the Active Directory setup to check for the necessary DNS entries.

After answering this question, the wizard prompts for the default permissions to be used for user and group objects as the following figure shows.

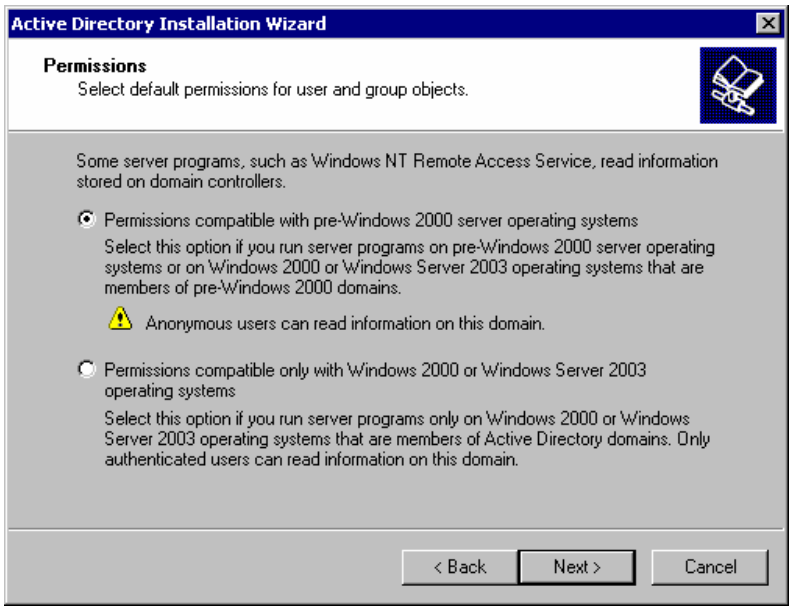

Active Directory Installation Wizard
Permissions
Select default permissions for user and group objects.
Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.
Permissions compatible with pre-Windows 2000 server operating systems
Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.
Anonymous users can read information on this domain.
Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems
Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.
< Back
Next >
Cancel

Figure 67. Permissions Compatibility dialog box

On servers running Windows NT Server 4.0 and earlier, read access for user and group information is assigned to anonymous users so that existing applications, including Microsoft BackOffice®, SQL Server, and some non–Microsoft applications, function correctly.

In Window 2000 and Windows Server 2003, members of the Anonymous Logon group have read access to this information only when the group is added to the Pre–Windows 2000 Compatible Access group.

Using the Active Directory Installation Wizard, you can choose if you want the Anonymous Logon group and the Everyone security groups to be added to the Pre–Windows 2000 Compatible Access group by selecting the **Permissions compatible with pre-Windows 2000 server operating systems** option. To prevent members of the Anonymous Logon group from gaining read access to user and group information, choose the **Permissions compatible only with Windows Server 2003 operating systems** option.

You can manually switch between the backward compatible and high-security settings on Active Directory objects by adding the Anonymous Logon security group to the pre-Windows 2000 Compatible Access security group using the Active Directory Users and Computers snap-in.

Choose the first option if there are other Windows NT 4.0 domain controllers and servers that still need to communicate with the Windows Server 2003 Active Directory domain. This option reduces security but is absolutely necessary if these servers exist. Choose the second option if no other Windows NT 4.0 domain controllers or servers exist. After making this selection, a dialog box asks for the Restore Mode password as the figure below shows.

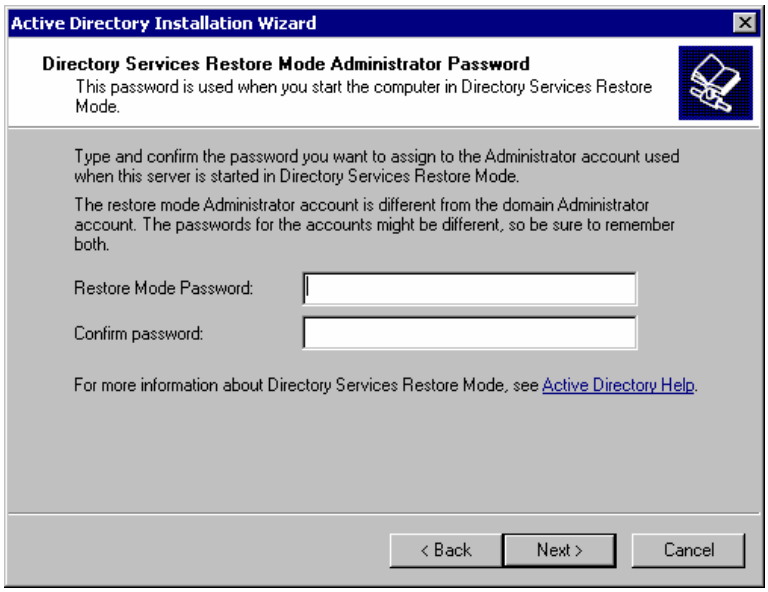

Active Directory Installation Wizard
Directory Services Restore Mode Administrator Password
This password is used when you start the computer in Directory Services Restore Mode.
Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.
The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.
Restore Mode Password:
Confirm password:
For more information about Directory Services Restore Mode, see Active Directory Help.
< Back
Next >
Cancel

Figure 68. Restore Mode Password dialog box

This password is used in the event of a major failure of the server. A special command line interface called Restore Mode can be invoked to troubleshoot issues with the failed server. This password is the one used to enter Restore Mode. After typing the Restore Mode password, the Summary screen appears as shown below. The user is asked to review the answers to questions presented during the wizard, confirm the selections, or go back and make necessary changes.

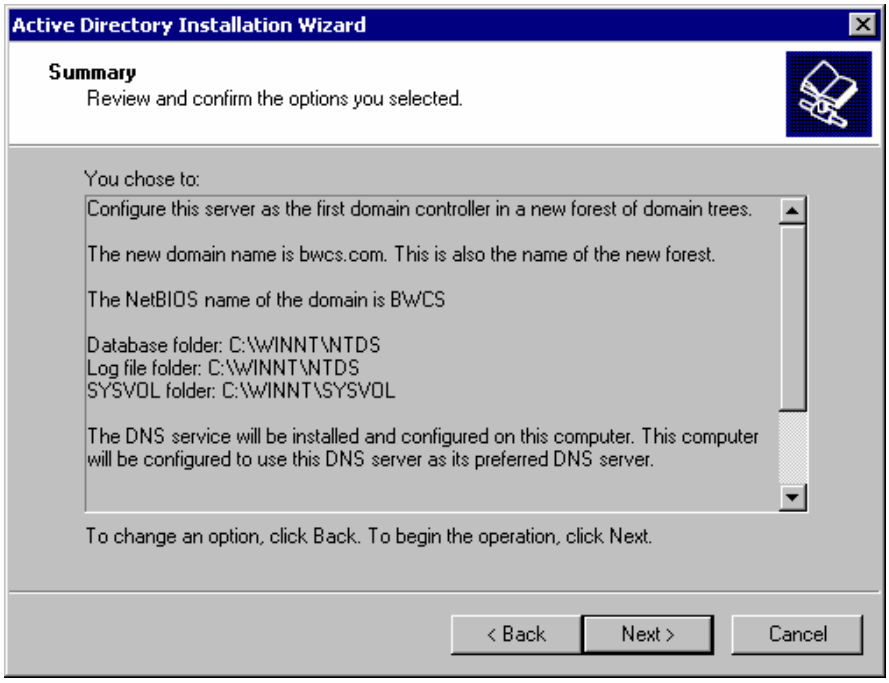

Active Directory Installation Wizard
Summary
Review and confirm the options you selected.
You chose to:
Configure this server as the first domain controller in a new forest of domain trees.
The new domain name is bwcs.com. This is also the name of the new forest.
The NetBIOS name of the domain is BWCS
Database folder: C:\WINNT\NTDS
Log file folder: C:\WINNT\NTDS
SYSVOL folder: C:\WINNT\SYSVOL
The DNS service will be installed and configured on this computer. This computer will be configured to use this DNS server as its preferred DNS server.
To change an option, click Back. To begin the operation, click Next.
< Back
Next >
Cancel

Figure 69. Summary dialog box

After clicking **Next**, the Active Directory Installation Wizard starts as the figure below shows.

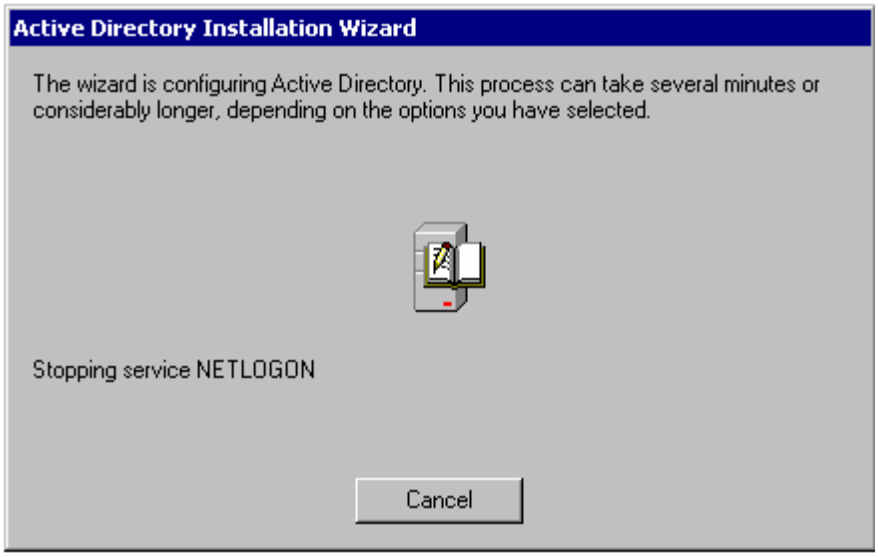

Active Directory Installation Wizard
The wizard is configuring Active Directory. This process can take several minutes or considerably longer, depending on the options you have selected.
Stopping service NETLOGON
Cancel

Figure 70. Active Directory installation in progress

During the Active Directory installation, the DNS service must be installed and configured as the following figure shows.

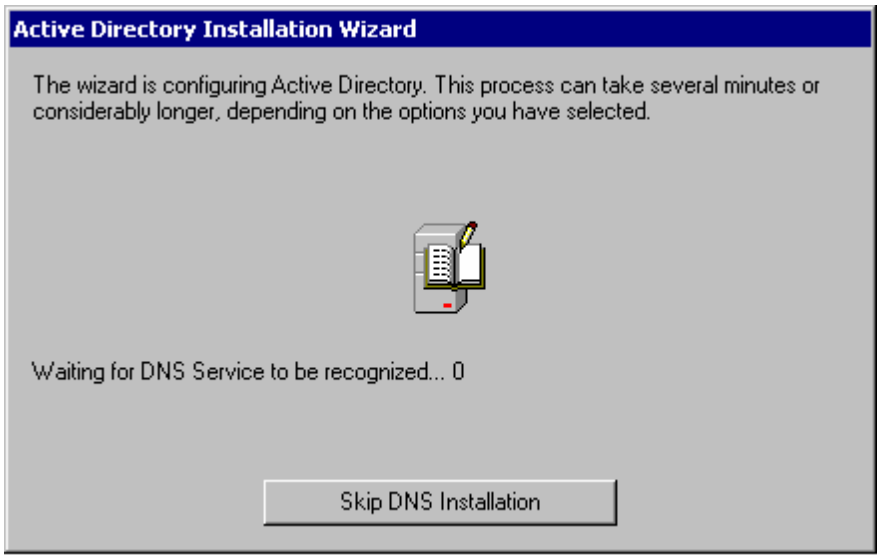

Active Directory Installation Wizard
The wizard is configuring Active Directory. This process can take several minutes or considerably longer, depending on the options you have selected.
Waiting for DNS Service to be recognized... 0
Skip DNS Installation

Figure 71. DNS installation during Active Directory installation

When installation has been completed, the wizard provides a summary as the following figure shows.

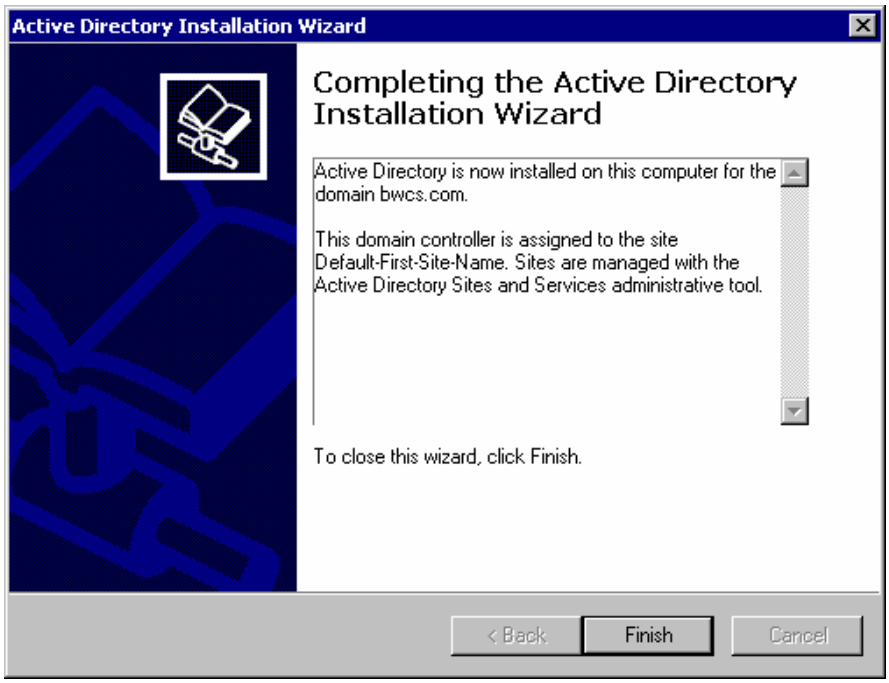

Active Directory Installation Wizard
Completing the Active Directory Installation Wizard
Active Directory is now installed on this computer for the domain bwcs.com.
This domain controller is assigned to the site Default-First-Site-Name. Sites are managed with the Active Directory Sites and Services administrative tool.
To close this wizard, click Finish.
< Back
Finish
Cancel

Figure 72. Summary of the installation results

After clicking **Finish**, the server must be rebooted, and then the system should be inspected to ensure Active Directory is functioning properly. The first thing to check is DNS. Use the DNS MMC snap-in to inspect the records created by Active Directory. It is not possible or necessary to know all the records created by Active Directory, but an administrator should know enough to make sure the correct types of records were created.

The following figure shows the DNS Administrator and the DNS records created by Active Directory.

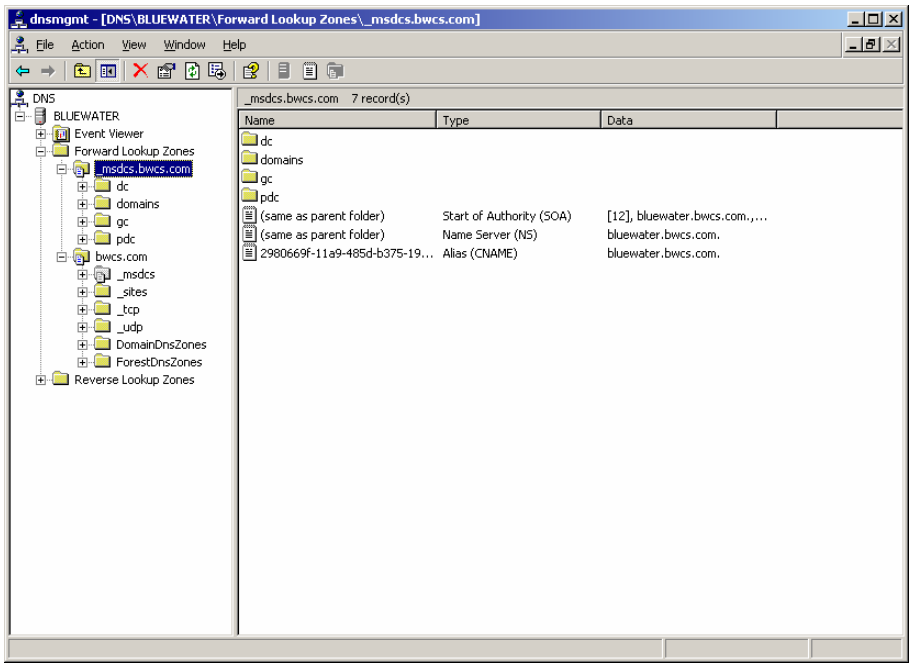


Figure 73. DNS Management snap-in showing Active Directory records

The records of most importance are found under the _msdcs.bwcs.com zone and _msdcs, _sites, _tcp, and _udp under the bwcs.com zone. These fundamental records enable Active Directory to function properly. A thorough check of the DNS server logs in Event Viewer also helps to confirm whether DNS is working properly.

Appendix B: Sample Log File from Compatibility Check

An option during installation of Windows Server 2003 is an automatic system compatibility test. If you select Check System Compatibility, Setup performs a comparison. The following output shows sample results from an in-place upgrade for a Windows NT PDC.

For more information about the sample in-place upgrade, see Sample In-Place Upgrade for a Windows NT PDC earlier in this document.

```
********************************************************************

                Windows Upgrade Compatibility

********************************************************************

Windows Setup cannot continue without service pack 5 or greater installed.
Please install the latest Windows NT 4.0 service pack.
================================================================================



Exchange Server
===============

The software for Microsoft Exchange Server 5.5 Standard Edition and Microsoft
Exchange Server 5.5 Enterprise Edition is not compatible with this version of
Microsoft Windows. You must install Exchange Server 5.5 Server Pack 3 or later in
order for these programs to run under this version of Windows.


For more information about this software and to download Exchange Server 5.5
Service Pack 3 or later, visit the manufacturers' web site at
http://www.microsoft.com/exchange.


For a list of software supported by this version of Windows, see the Microsoft
Windows Compatibility List at http://go.microsoft.com/fwlink/?LinkId=9946.




Microsoft Exchange 5.5
======================


The following software is not supported on this version of Microsoft Windows:


     Exchange 5.5
     Exchange 2000
     Site Server 3.0 (SP4 and below)
```

System Management Server 2.0 (SP2 and below)

Proxy Server

For more information about this software, see the Microsoft BackOffice Server page at http://www.microsoft.com/backofficeserver. Web addresses can change, so you might be unable to connect to this Web site.

For a list of software supported by this version of Windows, see the Microsoft Windows Compatibility List at http://go.microsoft.com/fwlink/?LinkId=9946.

Windows 95 and Windows NT 4.0 interoperability issues (Read Details!)

==========

Windows 95 and Windows NT 4.0 interoperability issues.

SUMMARY

Windows Server 2003 Domain Controllers implement default security settings that help prevent Domain Controller communications from being hijacked or otherwise tampered with. Certain down level machines are not capable of meeting these security requirements and thus cannot communicate with Windows Server 2003 Domain Controllers without administrative intervention.

Affected machines include Windows for Workgroups, Windows 95 machines that do not have the DS client pack installed, Windows NT 4.0 machines prior to Service Pack 4, and devices, including Pocket PC 2002 and previous versions, based on the Windows CE .NET version 4.1 or earlier.

SMB SIGNING

By default, Windows Server 2003 Domain Controllers require that all clients digitally sign SMB-based communications. The SMB protocol is used to provide file sharing, print sharing, various remote administration functions, and logon authentication for some down level clients. Windows for Workgroups, Windows 95 machines without the DS Client Pack, Windows NT 4.0 machines prior to Service Pack 3, and devices, including Pocket PC 2002 and previous versions, based on the Windows CE .NET version 4.1 or earlier are not capable of performing SMB signing and therefore cannot connect to Windows Server 2003 Domain Controllers by default. If such clients cannot be upgraded to a current operating system or upgraded to meet the minimum requirements described above, then the SMB signing requirement can be removed by disabling the following security policy in the Default Domain Controller GPO on the domain controllers OU:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft Network Server: Digitally sign communications (always)

Detailed instructions on how to modify this setting are provided below.

Warning: Disabling this security setting exposes all of your Domain Controller communications to "man in the middle" types of attacks. Therefore it is highly recommended that you upgrade your clients rather than disabling this security setting. The DS Client Pack, necessary for Windows 95 clients to perform SMB signing, can be obtained from the \clients\win9x subdirectory of the Windows 2000 Server CD.

SECURE CHANNEL SIGNING

By default, Windows Server 2003 Domain Controllers require that all secure channel communications be either signed or encrypted. Secure channels are used by Windows NT-based machines for communications between domain members and domain controllers as well as between domain controllers that have a trust relationship. Windows NT 4.0 machines prior to Service Pack 4 are not capable of signing or encrypting secure channel communications. If Windows NT 4.0 machines prior to SP4 must join this domain, or this domain must trust other domains that contain pre-SP4 Domain Controllers, then the secure channel signing requirement can be removed by disabling the following security policy in the Default Domain Controller GPO:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain Member: Digitally encrypt or sign secure channel data (always)

Detailed instructions on how to modify this setting are provided below.

Warning: Disabling this security setting exposes secure channel communications to "man in the middle" types of attacks. Therefore it is highly recommended that you upgrade your Windows NT 4.0 machines rather than disabling this security setting.

MODIFYING THE DEFAULT DOMAIN CONTROLLER GPO

To ensure all domain controllers are enforcing the same SMB and secure channel signing requirements, define the corresponding security settings in the Default Domain Controller GPO as follows:

1. Log on to a machine that has the Active Directory Users and Computers Snap-in installed.
2. Start --> Run --> DSA.MSC
3. Expand the Domain that contains your Windows Server 2003 Domain Controllers.
4. Right-click on the Domain Controllers OU and then click Properties.
5. Click the Group Policy tab, select the Default Domain Controller Policy, and then click Edit.
6. Expand Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options
7. In the result pane, double click the security option you want to modify. For example, Microsoft Network Server: Digitally sign communications (always) or Domain Member: Digitally encrypt or sign secure channel data (always).
8. Check the Define this policy setting box.
9. Disable or Enable the security setting as desired, and then select OK.

Appendix C: Related Links

See the following resources for further information:

- Windows Application Compatibility on the Windows Web site at http://www.microsoft.com/windows/appcompatibility/default.mspx
- Tools and Documentation for Upgrading to Windows Server 2003 on the Windows Server 2003 Web site at http://www.microsoft.com/windowsserver2003/upgrading/nt4/tooldocs/default.mspx
- How to: Set Up ADMT for a Windows NT 4.0-to-Windows Server 2003 Migration in the Microsoft Knowledge Base at http://support.microsoft.com/default.aspx?scid=kb;en-us;325851
- Migrating from Windows NT Server 4.0 to Windows Server 2003 in the Microsoft Download Center at http://www.microsoft.com/downloads/details.aspx?FamilyID=e92cf6a0-76f0-4e25-8de0-19544062a6e6&DisplayLang=en.
- Migrating Windows NT Server 4.0 Domains to Windows Server 2003 Active Directory on the Windows Server 2003 Web site at http://www.microsoft.com/windowsserver2003/evaluation/whyupgrade/nt4/nt4domtoad.mspx
- Upgrading Your Domain Controllers on the Windows Server 2003 Web site at http://www.microsoft.com/windowsserver2003/upgrading/nt4/domain/default.mspx
- Migrating ASP Pages to ASP.NET on the MSDN Web site at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/cpguide/html/cpconmigratingasppagestoasp.asp
- Windows Server 2003 Deployment Kit: Deploying Internet Information Services (IIS) 6.0 in the Microsoft Download Center at http://microsoft.com/downloads/details.aspx?FamilyId=F31A5FD5-03DB-46D2-9F34-596EDD039EB9&displaylang=en
- Windows XP home page at http://microsoft.com/windowsxp
- DNS and Microsoft Windows NT 4.0 on the Windows NT Server Web site at http://www.microsoft.com/ntserver/techresources/deployment/NTserver/dnswp.asp
- Designed for Windows logo program at http://www.microsoft.com/winlogo/default.mspx

For the latest information about Windows Server 2003, see the Windows Server 2003 Web site at http://www.microsoft.com/windowsserver2003.